













**Warsztat: Infoblox DNS Firewall & DNS Infoblox Threat Analytics.**  
Czyli jak w godzinę ochronić użytkowników.

Adam Obszyński  
SE CEE, [aobszynski@infoblox.com](mailto:aobszynski@infoblox.com)

# Housekeeping

Course Hours		Network Connectivity	
Parking		Phones/Computers	
Rest Rooms		Smoking	
Meals		Local Emergencies	
Fire Exits		Questions	

# Dzień dobry!



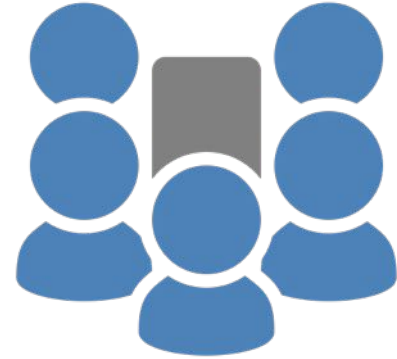
Rafał Szewczyk  
Regional Sales Manager Eastern Europe  
[rszewczyk@infoblox.com](mailto:rszewczyk@infoblox.com)  
+48 881 91 66 66



Adam Obszyński, CISSP, CCIE #8557  
Regional Sales Engineer Eastern Europe  
[aobszynski@infoblox.com](mailto:aobszynski@infoblox.com)  
+48 696 196 509

# Introductions

- Your name
- Your company, position, and responsibilities
- Previous experience
  - Security?
  - DNS?
  - DHCP?
  - Infoblox?
  - Networking?
- What do you want to get from this workshop?



# Agenda

- Wprowadzenie do Infoblox GRID
- **LAB1:** Tworzymy GRID, uruchamiamy usługi
- DNS<sup>3</sup> – zagrożenia
- **LAB2:** Sprawdzamy jak to działa na klasycznym DNS.
- DNS Firewall – jak to działa
- **LAB3:** Włączymy i sprawdzimy
- DNS Threat Analytics – jak to działa
- **LAB4:** Włączymy i sprawdzimy

# Agenda

- Wprowadzenie do Infoblox GRID
- **LAB1:** Tworzymy GRID, uruchamiamy usługi
- DNS<sup>3</sup> – zagrożenia
- **LAB2:** Sprawdzamy jak to działa na klasycznym DNS.
- DNS Firewall – jak to działa
- **LAB3:** Włączymy i sprawdzimy
- DNS Threat Analytics – jak to działa
- **LAB4:** Włączymy i sprawdzimy

# Lab Architecture

Subnet: 192.168.194.X

Mask: 255.255.255.0

Gateway: 192.168.194.1

POD #	IP == (X)	POD #	IP == (X)
1	.10 - 19	10	.100 - 109
2	.20 - 29	11	.110 - 119
3	.30 - 39	12	.120 - 129
4	.40 - 49	13	.130 - 139
5	.50 - 59	14	.140 - 149
6	.60 - 69	15	.150 - 159
7	.70 - 79	16	.160 - 169
8	.80 - 89	17	.170 - 179
9	.90 - 99	18	.180 - 189



**Grid Master**

nios-7.3.201....160G-2210.ova



**Reporting**

nios-7.3.201...300G-800.ova

URL: <https://192.168.194.xxx/ui/>

**L: admin**

**P: infoblox**

# LAB1: PC Preps

## Install DIG tool from ISC BIND (tools) package:

- Copy all files from **C:\INFOBLOX.LABS\dig\** to **C:\Windows\System32\**
- Copy **resolv.conf** file from **C:\INFOBLOX.LABS** to **C:\Windows\System32\drivers**

## Import Infoblox OVF images to VMWare Workstation

- **VMware Workstation -> File -> Open**
- OVA Images location: **C:\INFOBLOX.LABS\NIOS\_7.3.201**
- **GRID Master:** nios-7.3.201-329349-2016-05-24-18-24-38-**160G-2210**.ova
- **Reporting:** nios-7.3.201-329349-2016-05-24-18-24-38-**300G-800**.ova

## Tune VMs

- Under “**Edit virtual machine settings**” please change memory to:
- Grid Master (160G-2210): from 12GB to 8GB
- Reporting (300G-800) from 8GB to 4GB



# LAB1: Licenses

#1 Login via VMWare console to each NIOS VM Appliances

Login: **admin** password: **infoblox**

#2 Use “**set temp\_license**” command to generate temporary licenses.

Details on next slide.

#3 Login again.

Use “**set network**” command to configure IP addresses.

**192.168.194.xxx** mask 255.255.255.0 gateway 192.168.194.1

#4 Login to GRID Master <https://192.168.194.xxx/ui/>

# LAB1: Licenses

GRID Master: 2, 12, 17, 8

```
Infoblox > set temp_license
```

1. DNSone (DNS, DHCP)
2. DNSone with Grid (DNS, DHCP, Grid)
3. Network Services for Voice (DHCP, Grid)
4. Add DNS Server license
5. Add DHCP Server license
6. Add Grid license
7. Add Microsoft management license
8. Add vNIOs license
9. Add Multi-Grid Management license
10. Add Query Redirection license
11. Add Load Balancer license
12. Add Response Policy Zones license
13. Add FireEye license
14. Add DNS Traffic Control license
15. Add Cloud Network Automation license
16. Add Security Ecosystem license
17. Add Threat Analytics license

```
Select license (1-17) or q to quit: _
```

Reporting: 1, 3, 2

```
Infoblox > set temp_license
```

1. Add Grid license
2. Add vNIOs license
3. Add Reporting license

```
Select license (1-3) or q to quit: _
```

# LAB1: set network

Subnet: 192.168.194.X

Mask: 255.255.255.0

Gateway: 192.168.194.1

```
Infoblox > show network
Current LAN1 Network Settings:
IPv4 Address:      192.168.1.2
Network Mask:     255.255.255.0
Gateway Address:  192.168.1.1
HA enabled:       false
Grid Status:     Master of Infoblox Grid
Infoblox > _
```

POD #	IP == (X)	POD #	IP == (X)
1	.10 - 19	10	.100 - 109
2	.20 - 29	11	.110 - 119
3	.30 - 39	12	.120 - 129
4	.40 - 49	13	.130 - 139
5	.50 - 59	14	.140 - 149
6	.60 - 69	15	.150 - 159
7	.70 - 79	16	.160 - 169
8	.80 - 89	17	.170 - 179
9	.90 - 99	18	.180 - 189

```
Infoblox > set network
NOTICE: All HA configuration is performed from the GUI. This interface is
used only to configure a standalone node or to join a Grid.
Enter IP address: 192.168.0.130
Enter netmask [Default: 255.255.255.0]:
Enter gateway address [Default: 192.168.0.1]:
Configure IPv6 network settings? (y or n): n
Become grid member? (y or n): n

New Network Settings:
IPv4 address:      192.168.0.130
IPv4 Netmask:     255.255.255.0
IPv4 Gateway address: 192.168.0.1

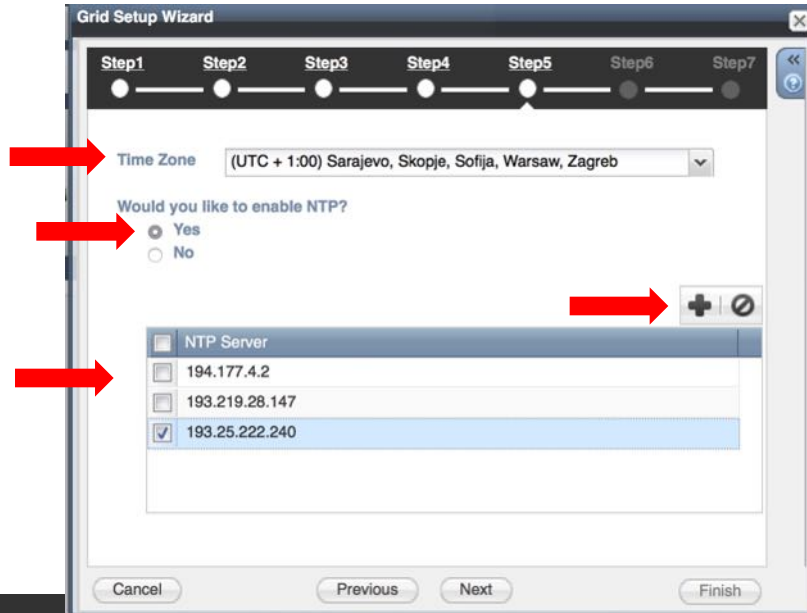
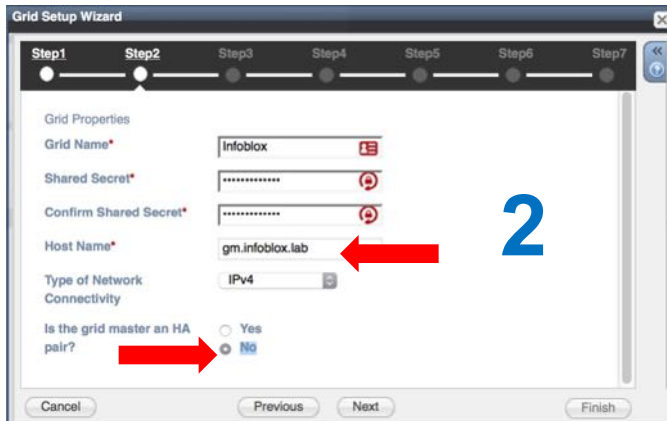
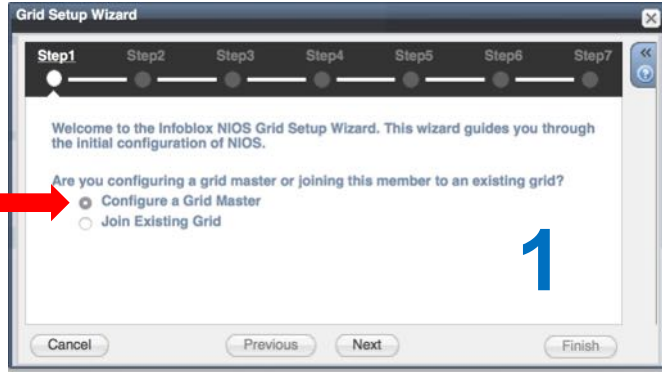
Old IPv4 Network Settings:
IPv4 address:      192.168.1.2
IPv4 Netmask:     255.255.255.0
IPv4 Gateway address: 192.168.1.1
Is this correct? (y or n): y
Are you sure? (y or n): y
Network settings have been updated.

Good Bye
[2016/06/03 13:59:48.012] System restart...
_
```

# LAB1: GM INIT

L: admin P: infoblox

<https://192.168.194.xxx/ui>



# LAB1: Add Member (Reporting)

GRID -> Grid Manager -> Members



or



1

Add Grid Member > Step 1 of 3

Member Type: Virtual NIOS

Host Name\*: tr.infoblox.lab Must be a fully qualified domain name

Time Zone: (UTC + 1:00) Sarajevo, Override

Inherited from Grid Infoblox

Comment:

Master Candidate:

Cancel Previous Next Save & Close

2

Add Grid Member > Step 2 of 3

Type of Network Connectivity: IPv4

Type of Member:

- Standalone Member
- High Availability Pair

Required Ports and Addresses

Interface	Address	Subnet Mask (I...	Gateway	VL...	Port Settings
LAN1 (IPv4)	192.168.0.131	255.255.255.0	192.168.0.1		Automatic

Cancel Previous Next Save & Close

3






	Name	HA	Status	IPv4 Address
	gm.infoblox.lab	No	Running	192.168.0.130
	tr.infoblox.lab	No	Offline	192.168.0.131

# LAB1: Add Member (Reporting)

Login to **Reporting Appliance** console or use its WEB GUI  
Join Reporting member to GRID Master.

```
Infoblox > set membership ←
Join status: No previous attempt to join a grid.
Enter New Grid Master VIP: 192.168.0.130
Enter Grid Name [Default Infoblox]:
Enter Grid Shared Secret: test
Join grid as member with attributes:
  Grid Master VIP: 192.168.0.130 ←
  Grid Name: Infoblox
  Grid Shared Secret: test ←

WARNING: Joining a grid will replace all the data on this node!
Is this correct? (y or n): y ←
Are you sure? (y or n): _
```

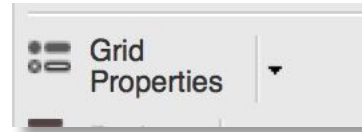
	Name	HA	Status	IPv4 Address	IP
	 gm.infoblox.lab	No	Running	192.168.0.130	
	 tr.infoblox.lab	No	Running	192.168.0.131	

# LAB1: Session Timeout

Login to **GM web GUI**

**GRID**

**Grid Properties on the right:**



**Security (on the left)**

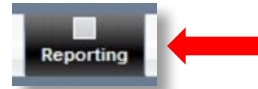
**Set “Session Timeout (s)\*” to 99999**



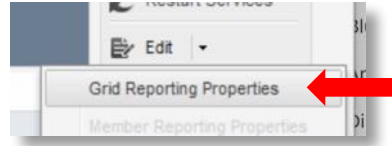
# LAB1: Enable Reporting

Login to **GM web GUI**

**GRID -> Grid Manager -> Reporting**



**Grid Reporting Properties on the right:**



Check **Enable Data Indexing:**

**Enable all categories**

And make total **100%**



Save

Restart Services



# Agenda

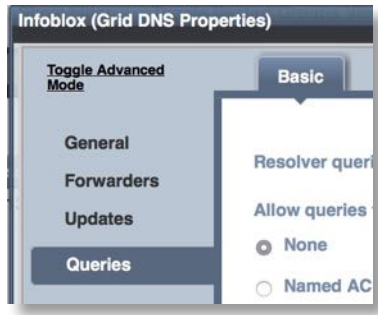
- Wprowadzenie do Infoblox GRID
- **LAB1:** Tworzymy GRID, uruchamiamy usługi
- **DNS^3 – zagrożenia**
- **LAB2:** Sprawdzamy jak to działa na klasycznym DNS.
- DNS Firewall – jak to działa
- **LAB3:** Włączymy i sprawdzimy
- DNS Threat Analytics – jak to działa
- **LAB4:** Włączymy i sprawdzimy

# Agenda

- Wprowadzenie do Infoblox GRID
- **LAB1:** Tworzymy GRID, uruchamiamy usługi
- DNS<sup>3</sup> – zagrożenia
- **LAB2:** Sprawdzamy jak to działa na klasycznym DNS.
- DNS Firewall – jak to działa
- **LAB3:** Włączymy i sprawdzimy
- DNS Threat Analytics – jak to działa
- **LAB4:** Włączymy i sprawdzimy

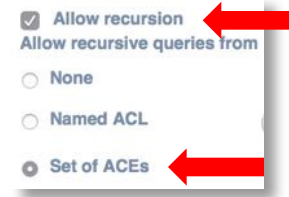
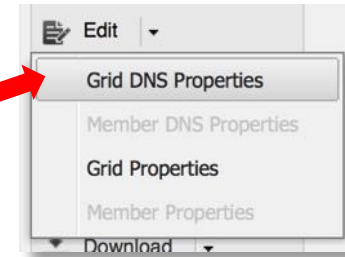
# LAB2: Classical DNS

Login to GM WEB GUI <https://gmipaddress/ui/>  
Change DNS settings to allow Recursive queries.  
GRID -> Grid Manager-> DNS  
On the right: EDIT -> Grid DNS Properties

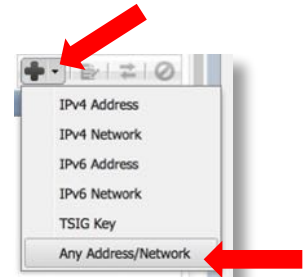


Go into **Queries** tab  
and check **Allow recursion**

Check **Set of ACEs**



Next to “+” select **triangle** and **Any Address/Network**



# LAB2: Classical DNS

Login to GM WEB GUI <https://gmipaddress/ui/>  
GRID -> Grid Manager-> DNS

The screenshot shows the Infoblox Grid Manager web interface. The top navigation bar includes 'Dashboards', 'Data Management', 'Smart Folders', 'Reporting', and 'Grid'. A red arrow points to the 'Grid' tab. Below this, the 'Grid Manager' section has sub-tabs for 'Upgrade', 'Licenses', and 'HSM Group'. A red arrow points to the 'Grid Manager' tab. Underneath, there are service icons for 'DHCP', 'DNS', 'HTTP (File Dist)', 'FTP', 'NTP', 'bloxTools', and 'Captive Portal'. A red arrow points to the 'DNS' icon. Below the icons, there are sections for 'Members' and 'Services'. The 'DNS' service is selected, showing a 'Quick Filter' set to 'None', a 'Filter On' status of 'Off', and a 'Group By' dropdown set to 'Choose one'. At the bottom, there is a 'Go to' search bar and a table with the following data:

Name	Service Status	IPv4 Address	Comment	Site
gm.infoblox.la	Not Running	192.168.0.130		

This is a close-up of the table from the previous screenshot. It shows a search bar at the top with a 'Go' button and a toolbar with icons for refresh, play, stop, and print. The table has the following data:

Name	Service Status	IPv4 Address	Comment	Site
<input checked="" type="checkbox"/> gm.infoblox.la	Not Running	192.168.0.130		

This is another close-up of the table, showing the service status updated. The 'Service Status' cell is highlighted in green and contains the text 'DNS Service is working'. A red arrow points to this cell.

Name	Service Status	IPv4 Address
<input type="checkbox"/> gm.infoblox.la	DNS Service is working	192.168.0.130

# LAB2: Classical DNS

Change your DNS setting in Windows – point to your GM IP address

Edit file **resolv.conf** in **C:\Windows\System32\drivers\etc\** directory.  
Change 8.8.8.8 to your GM IP address.

Test DNS service with “DIG” command or nslookup if you prefer to use it.

```
dig @192.168.0.130 infoblox.com
```



```
;; ANSWER SECTION:
infoblox.com.      3600    IN      A       54.235.223.101

;; Query time: 300 msec
;; SERVER: 192.168.0.130#53(192.168.0.130)
;; WHEN: Fri Jun 03 23:26:06 Central European Daylight Time 2016
;; MSG SIZE rcvd: 57
```



# LAB2: Malware & Data Exfiltration

## Few queries:

dig @192.168.0.130 lovemydress.pl

dig @192.168.0.130 brt2014.com

dig @192.168.0.130 all-that-and-more.net

## Few more to try:

<http://www.ignoremydata.com/>

# Agenda

- Wprowadzenie do Infoblox GRID
- **LAB1:** Tworzymy GRID, uruchamiamy usługi
- DNS<sup>3</sup> – zagrożenia
- **LAB2:** Sprawdzamy jak to działa na klasycznym DNS.
- **DNS Firewall – jak to działa**
- **LAB3:** Włączymy i sprawdzimy
- DNS Threat Analytics – jak to działa
- **LAB4:** Włączymy i sprawdzimy

# Agenda

- Wprowadzenie do Infoblox GRID
- **LAB1:** Tworzymy GRID, uruchamiamy usługi
- DNS<sup>3</sup> – zagrożenia
- **LAB2:** Sprawdzamy jak to działa na klasycznym DNS.
- DNS Firewall – jak to działa
- **LAB3:** Włączymy i sprawdzimy
- DNS Threat Analytics – jak to działa
- **LAB4:** Włączymy i sprawdzimy



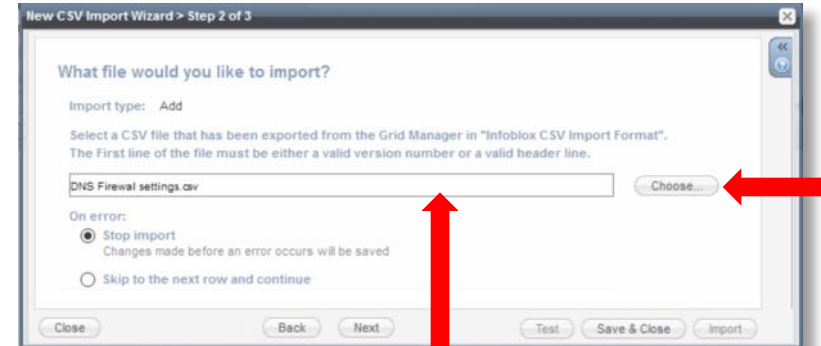
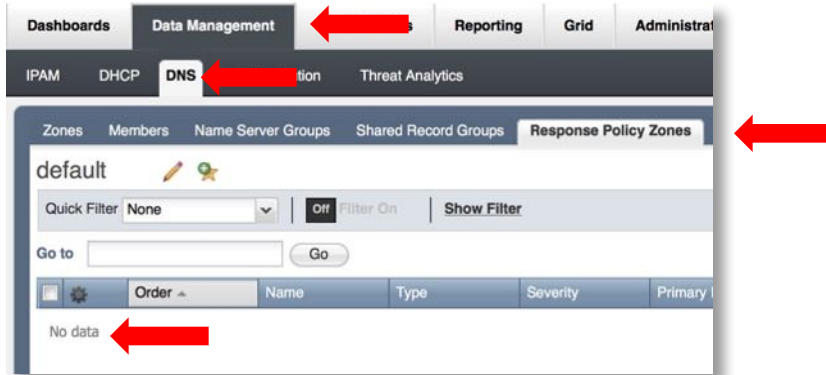
# LAB3: DNS Firewall



Login to GM WEB GUI <https://gmipaddress/ui/>

Enable DNS Firewall – RPZ Rules.

Data Management -> DNS -> Response Policy Zones



On the right – Click on **CSV Import**:



On Step 2 screen click **Choose** and select **DNS Firewall CSV** file from **C:\INFOBLOX.LABS\**

Then Restart services:



and check Syslog for RPZ AXFRs.

# LAB3: Malware & Data Exfiltration

## Few queries:

dig @192.168.0.130 lovemydress.pl

dig @192.168.0.130 brt2014.com

dig @192.168.0.130 all-that-and-more.net

## Check Syslog

Check Dashboards -> Status -> Security

# Agenda

- Wprowadzenie do Infoblox GRID
- **LAB1:** Tworzymy GRID, uruchamiamy usługi
- DNS<sup>3</sup> – zagrożenia
- **LAB2:** Sprawdzamy jak to działa na klasycznym DNS.
- DNS Firewall – jak to działa
- **LAB3:** Włączymy i sprawdzimy
- **DNS Threat Analytics – jak to działa**
- **LAB4:** Włączymy i sprawdzimy

# Agenda

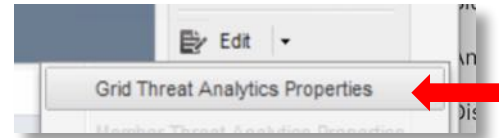
- Wprowadzenie do Infoblox GRID
- **LAB1:** Tworzymy GRID, uruchamiamy usługi
- DNS<sup>3</sup> – zagrożenia
- **LAB2:** Sprawdzamy jak to działa na klasycznym DNS.
- DNS Firewall – jak to działa
- **LAB3:** Włączymy i sprawdzimy
- DNS Threat Analytics – jak to działa
- **LAB4:** Włączymy i sprawdzimy

# LAB4: DNS Threat Analytics

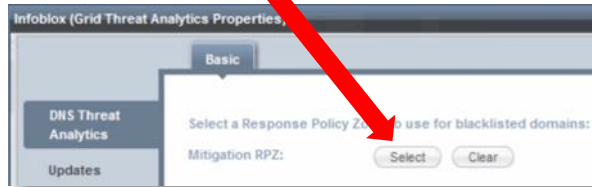
Login to GM WEB GUI <https://gmipaddress/ui/>  
GRID -> Grid Manager -> Threat Analytics



On the right: Edit -> Grid Threat Analytics Properties

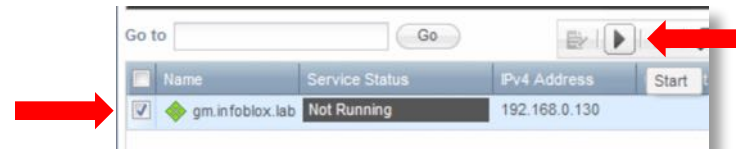


Click **Select** and select "threat-analytics"

A screenshot of a dropdown menu showing three options: "blacklist", "threat-analytics" (highlighted), and "whitelist". A red arrow points to the "threat-analytics" option.

Name	Comment	Site
blacklist		
threat-analytics		
whitelist		

Enable DNS Threat Analytics



# LAB4: Malware & Data Exfiltration

Let's play:

<http://www.ignoremydata.com/>

**Check Syslog**

**Check Dashboards -> Status -> Security**

# Agenda

- Wprowadzenie do Infoblox GRID
  - **LAB1:** Tworzymy GRID, uruchamiamy usługi
  - DNS<sup>3</sup> – zagrożenia
  - **LAB2:** Sprawdzamy jak to działa na klasycznym DNS.
  - DNS Firewall – jak to działa
  - **LAB3:** Włączymy i sprawdzimy
  - DNS Threat Analytics – jak to działa
  - **LAB4:** Włączymy i sprawdzimy
- **Koniec**