

# CYBERSTARTER

Co w hostach piszczy, czyli jak ogarnąć monitoring infrastruktury i mieć czas na CSa

Michał Franczak

**OPEN SOURCE SOC**

# OPEN SOURCE SOC

Nagios: CIA

# OPEN SOURCE SOC

Nagios: CIA

Open Source != Za darmo

# DZIŚ BĘDZIE

- Nagios XI + Centreon
- Hosty: Windows i Linux
- SNMP
- NSClient++ i NRPE

# DZIŚ NIE BĘDZIE

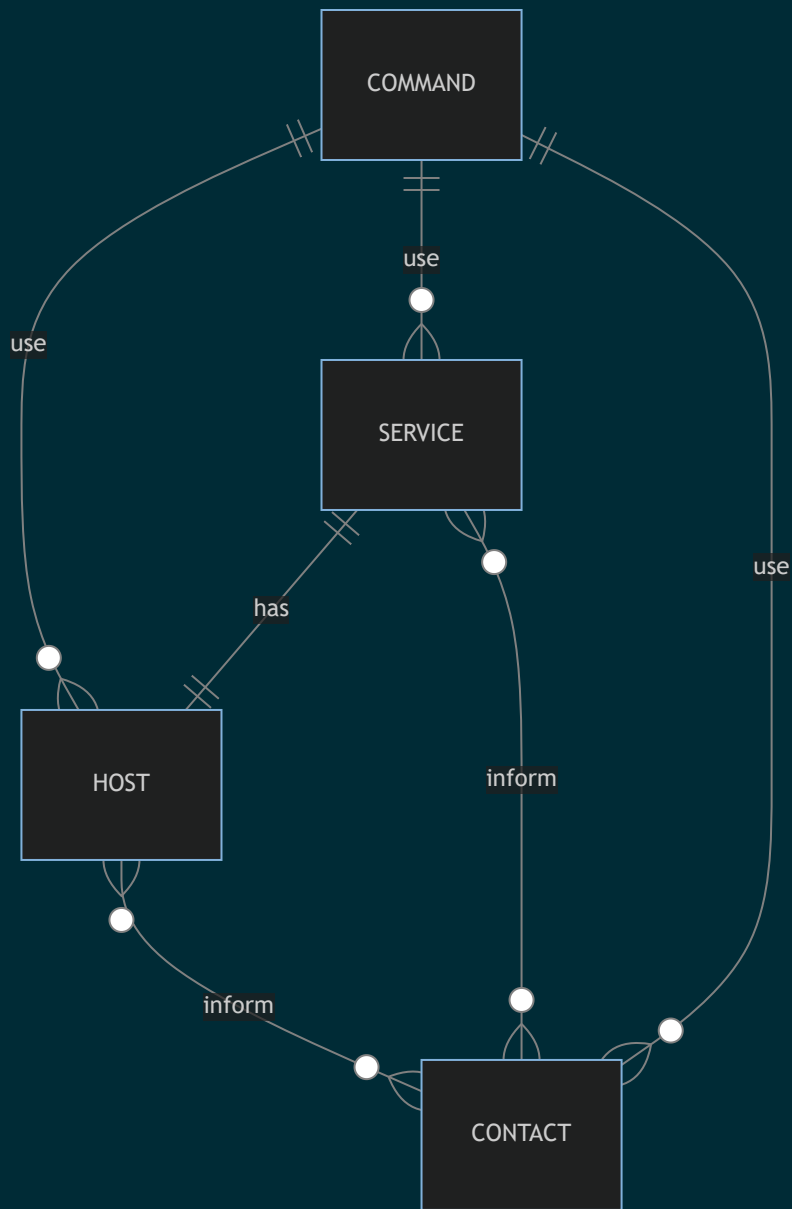
- Urządzeń sieciowych
- IoT oraz MiB
- Szablonów
- Dashboardów i raportów
- Trybu pasywnego

# PODSTAWOWE KONFIGURACJE W NAGIOSIE

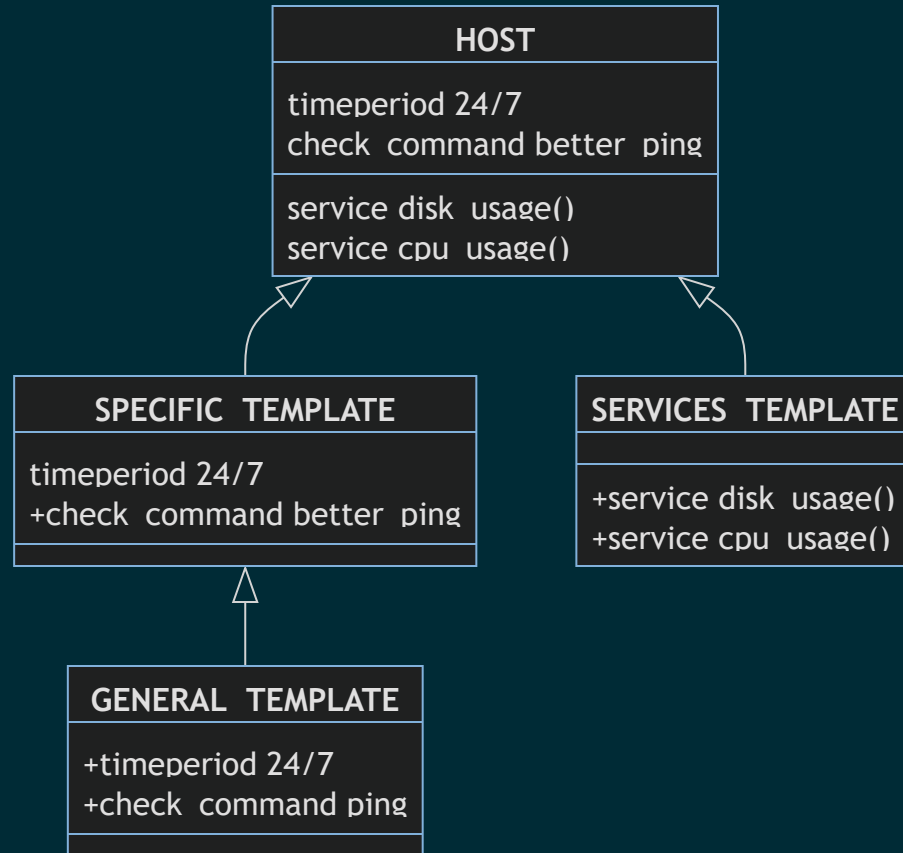
```
define host{
    host_name          bogus-router
    alias              Bogus Router #1
    address            192.168.1.254
    parents            server-backbone
    check_command       check-host-alive
    check_interval      5
    retry_interval      1
    max_check_attempts 5
    check_period        24x7
    process_perf_data   0
    retain_nonstatus_information 0
}
```

# PODSTAWOWE KONFIGURACJE W NAGIOSIE



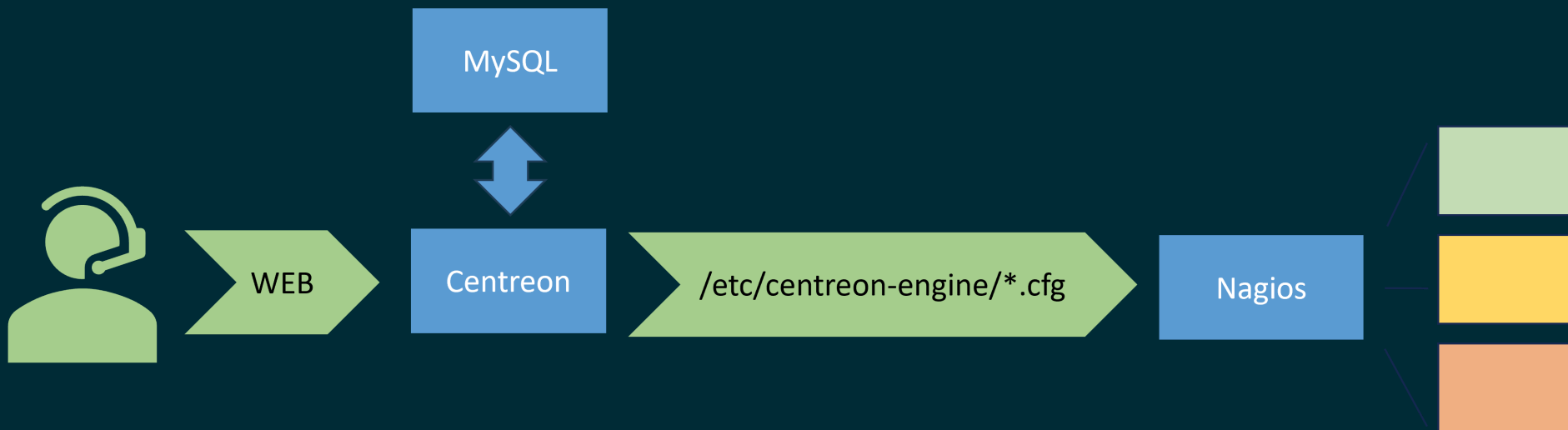


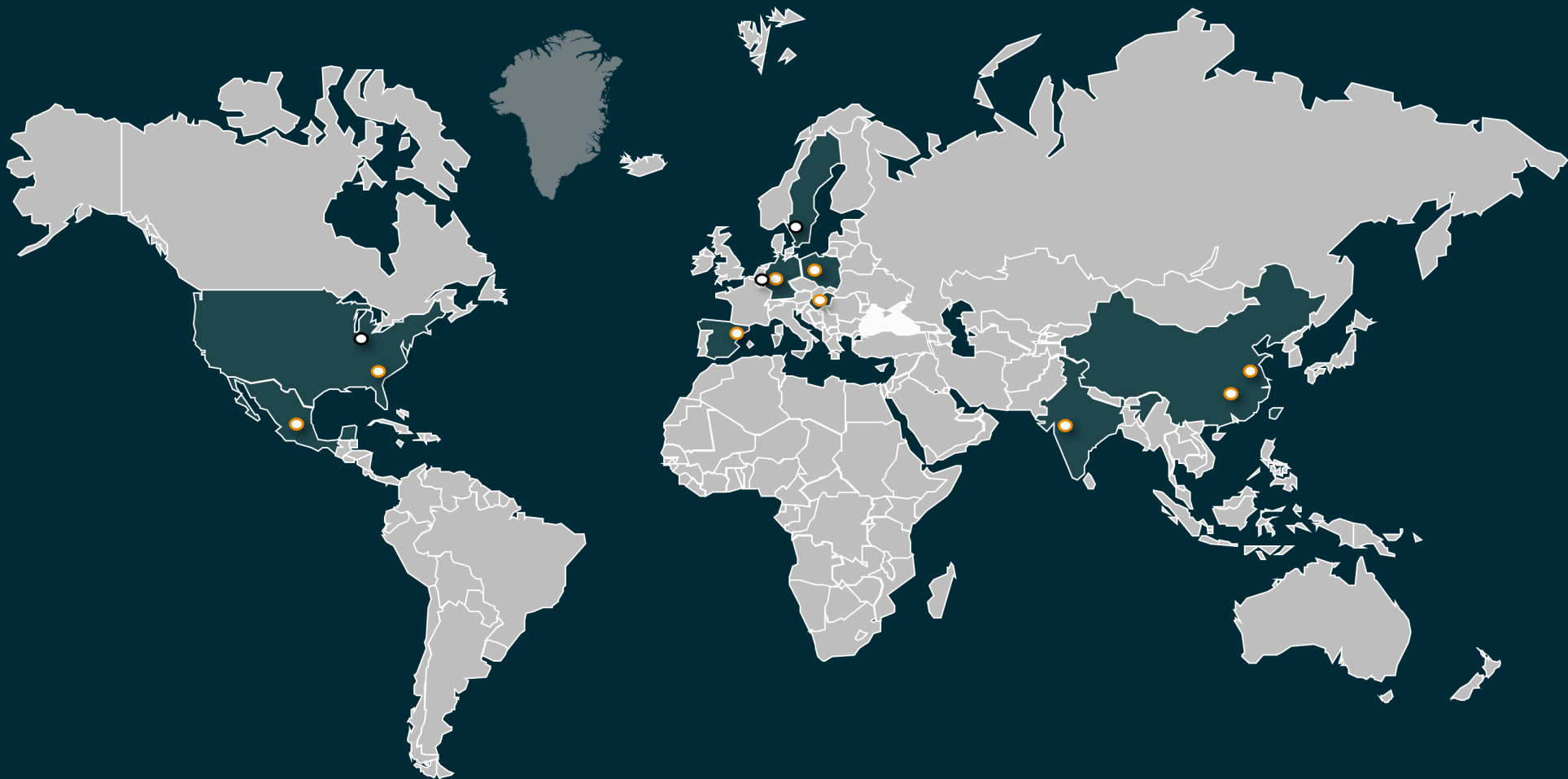
# PODSTAWOWE KONFIGURACJE W NAGIOSIE

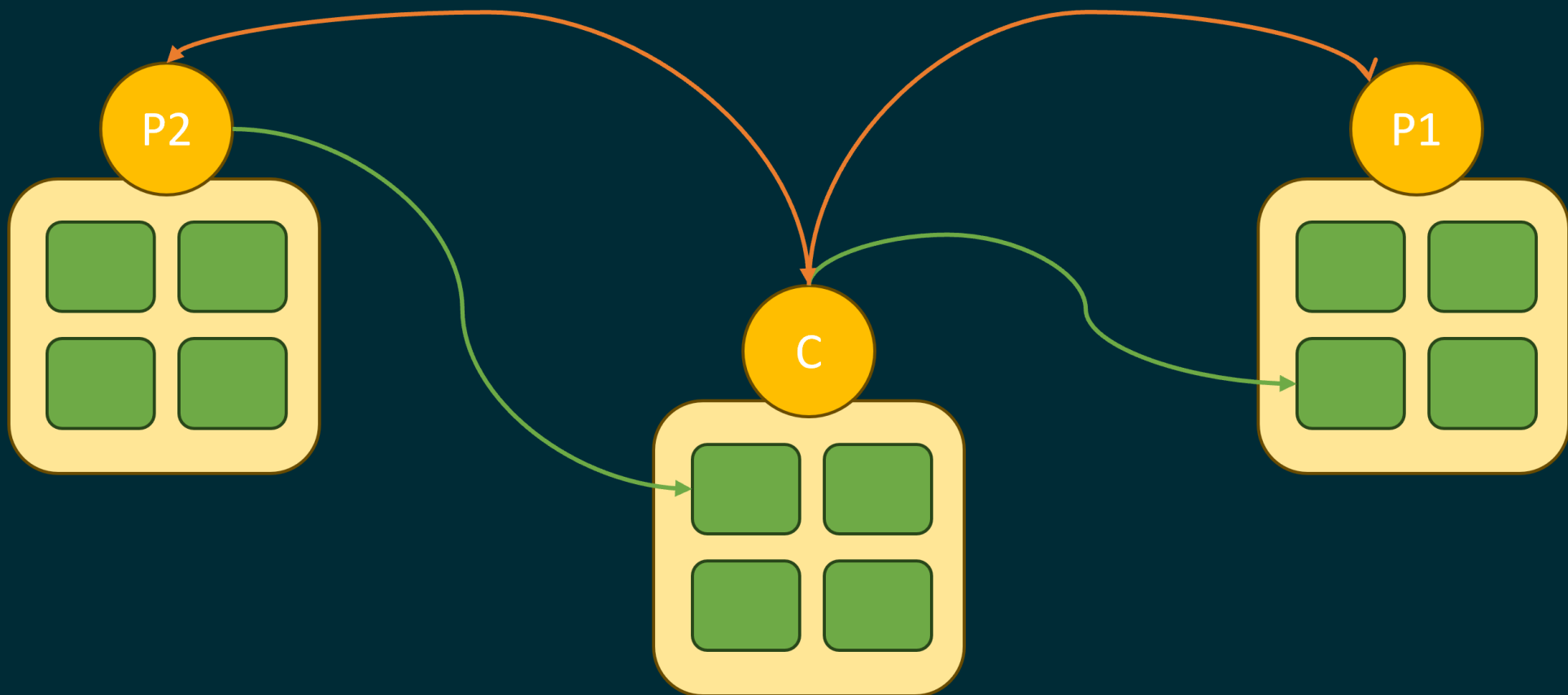


# INNE

- grupa hostów / usług
- eskalacje
- grupy kontkatów
- zależności







Poller

Search

Filters

+ Add



















+ Add (advanced)

Export configuration

Duplicate

Delete

30

<input type="checkbox"/>	Name	IP Address	Server type	Is running ?	Conf Changed *	PID	Uptime	Last Update	Version	Default	Status	Actions	Options
<input type="checkbox"/>	Central	127.0.0.1	Central	YES	NO	24413	18 days	November 6, 2024 10:30:16 AM	Centreon Engine 22.10.9	Yes	ENABLED	 	 1
<input type="checkbox"/>	POLLER-INDIEN	192.168.1.10	Distant Poller	YES	NO	752	24 days	November 6, 2024 10:30:22 AM	Centreon Engine 22.10.7	No	ENABLED	 	 1
<input type="checkbox"/>	POLLER-MEXICO	192.168.1.11	Distant Poller	YES	NO	639	77 days	November 6, 2024 10:30:25 AM	Centreon Engine 22.10.9	No	ENABLED	 	 1
<input type="checkbox"/>	POLLER-POLEN	192.168.1.12	Distant Poller	YES	NO	4422	83 days	November 6, 2024 10:30:37 AM	Centreon Engine 22.10.10	No	ENABLED	 	 1
<input type="checkbox"/>	POLLER-SPANIEN	192.168.1.13	Distant Poller	YES	NO	1998	96 days	November 6, 2024 10:30:14 AM	Centreon Engine 22.10.2	No	ENABLED	 	 1
<input type="checkbox"/>	POLLER-UNGARN	192.168.1.14	Distant Poller	YES	NO	14507	74 days	November 6, 2024 10:30:44 AM	Centreon Engine 22.10.6	No	ENABLED	 	 1

**WSZYSTKO ZACZYNA SIĘ NA PAPIERZE**



# WSZYSTKO ZACZYNA SIĘ NA PAPIERZE

- Klasyfikacja / szacowanie ryzyka

# WSZYSTKO ZACZYNA SIĘ NA PAPIERZE

- Klasyfikacja / szacowanie ryzyka
- Specyficzne wymagania

# WSZYSTKO ZACZYNA SIĘ NA PAPIERZE

- Klasyfikacja / szacowanie ryzyka
- Specyficzne wymagania
- Działająca infrastruktura

# WSZYSTKO ZACZYNA SIĘ NA PAPIERZE

- Klasyfikacja / szacowanie ryzyka
- Specyficzne wymagania
- Działająca infrastruktura
- Inne narzędzia

# WSZYSTKO ZACZYNA SIĘ NA PAPIERZE

- Klasyfikacja / szacowanie ryzyka
- Specyficzne wymagania
- Działająca infrastruktura
- Inne narzędzia
- Polityki, zasady, normy, uzgodnienia

# **ANALIZA PRZYPADKU**

# ANALIZA PRZYPADKU

- Czy wystarczy informacja, że host żyje

# ANALIZA PRZYPADKU

- Czy wystarczy informacja, że host żyje
- Jakie usługi i z której strony



# ANALIZA PRZYPADKU

- Czy wystarczy informacja, że host żyje
- Jakie usługi i z której strony
- Skąd monitorować

# ANALIZA PRZYPADKU

- Czy wystarczy informacja, że host żyje
- Jakie usługi i z której strony
- Skąd monitorować
- Jakież szczegóły / parametry / dane?

# ANALIZA PRZYPADKU

- Czy wystarczy informacja, że host żyje
- Jakie usługi i z której strony
- Skąd monitorować
- Jakież szczegóły / parametry / dane?
- Kto, jak i kiedy ma być informowany?

**~~SKY~~ SHELL IS THE LIMIT**

**PORA NA CS'A**

# PORA NA CS'A

Case Study

# CS:DEBIAN

- Host alive - PING
- SNMP
  - CPU i średnie obciążenie
  - Pamięć i swap
  - Proces NGINX
- Service HTTP
- Specyficzne dane w DB

# SNMP AGENT NA LINUXSIE

```
agentaddress 0.0.0.0
com2sec notConfigUser default cyberstarter
view centreon included .1.3.6.1
view systemonly included .1.3.6.1.2.1.1
view systemonly included .1.3.6.1.2.1.25.1
access notConfigGroup "" any noauth exact centreon none none
access notConfigGroup "" any noauth exact systemview none none
```



# SNMP AGENT NA LINUXSIE

```
snmpwalk -v2c -ccyberstarter 192.168.0.103 .1.3.6.1.2.1.25.4.2.1.2
```

# CS:WINDOWS SERVER

- Host alive - PING
- SNMP
  - CPU
  - Pamięć
  - Dysk
- check\_nrpe -> NSClient++
  - Usługi i procesy
  - Jakość pliku backupu

# **BARDZO DZIĘKUJĘ ZA UWAGĘ**

Michał Franczak

rahn@stricte.net

[https://github.com/rahnidos/cyberstarter2024\\_monitori](https://github.com/rahnidos/cyberstarter2024_monitori)