CYBERSTARTER

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

Michał Franczak

OPEN SOURCE SOC

Nagios: CIA

Open Source != Za darmo

DZIŚ BĘDZIE

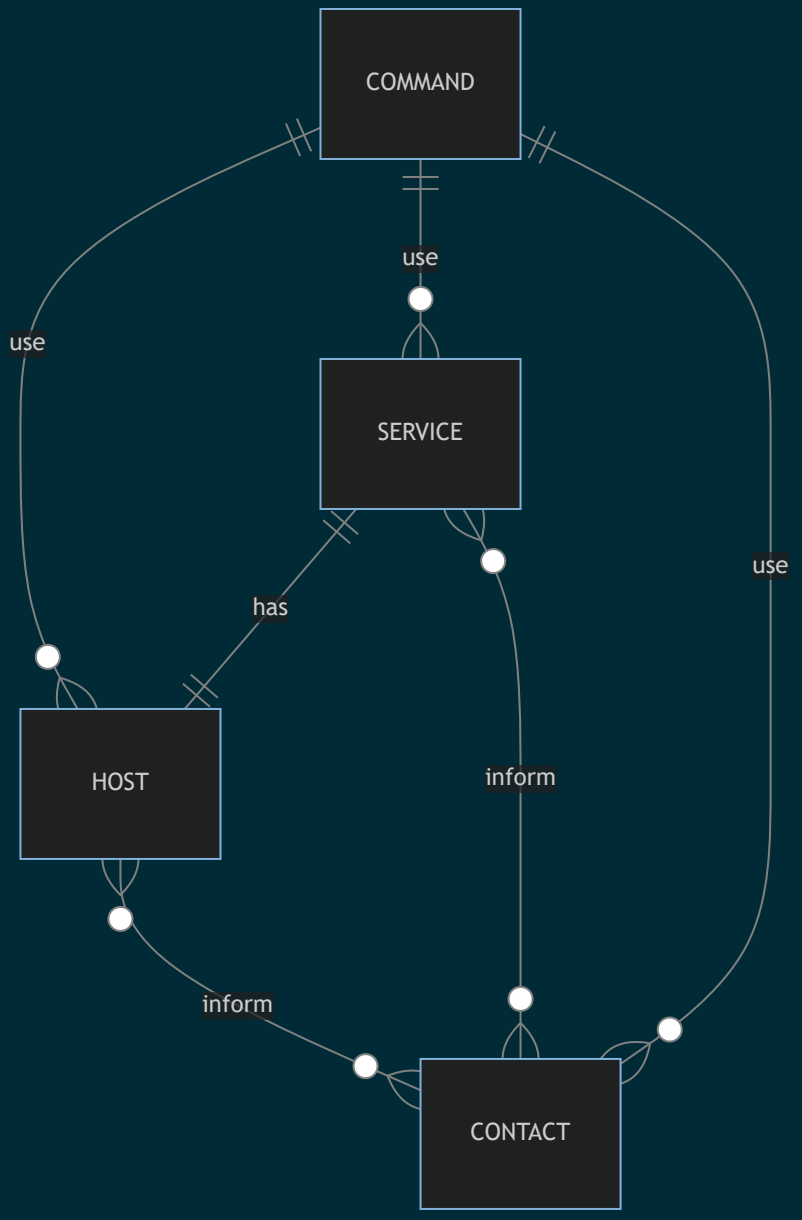
- Nagios XI + Centreon
- Hosty: Windows i Linux
- SNMP
- NSClient++ i NRPE

DZIŚ NIE BĘDZIE

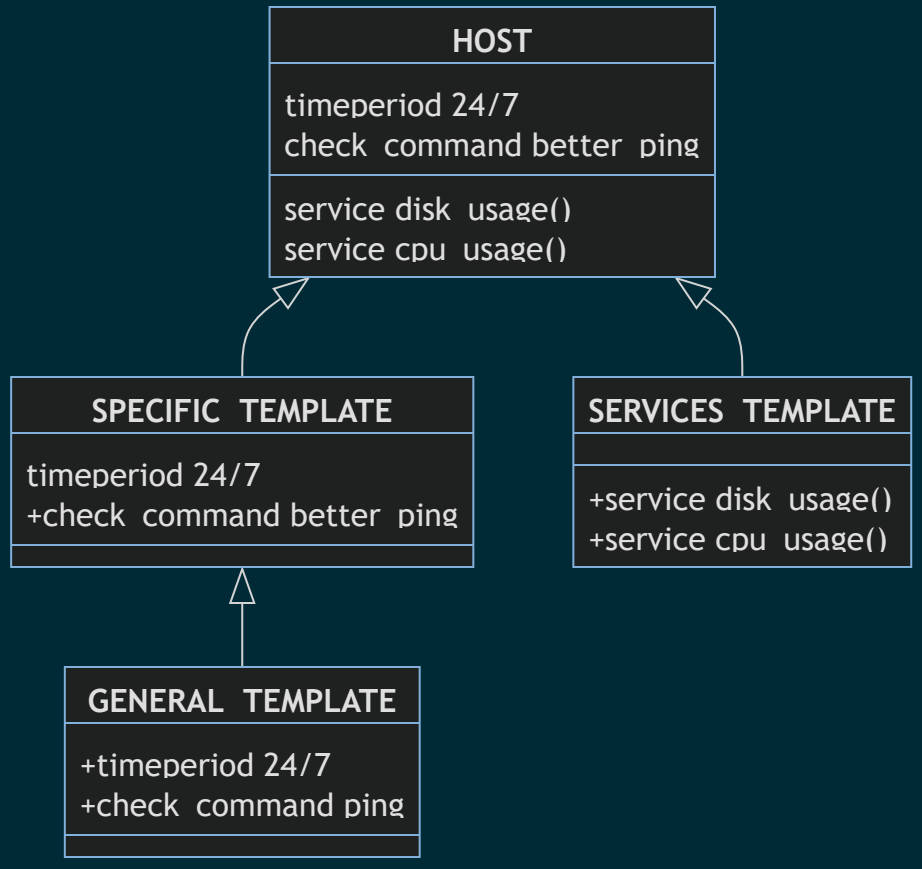
- Urządzeń sieciowych
- IoT oraz MiB
- Szablonów
- Dashboardów i raportów
- Trybu pasywnego

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
  }
```

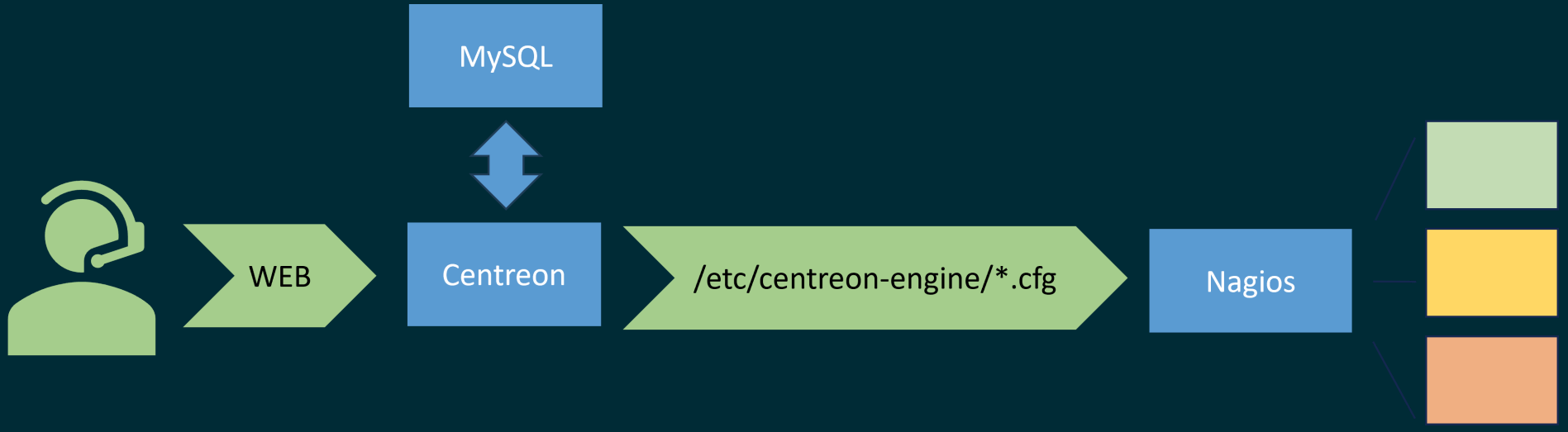

COMMAND
use
use
use
SERVICE
has
HOST
inform
inform
CONTACT

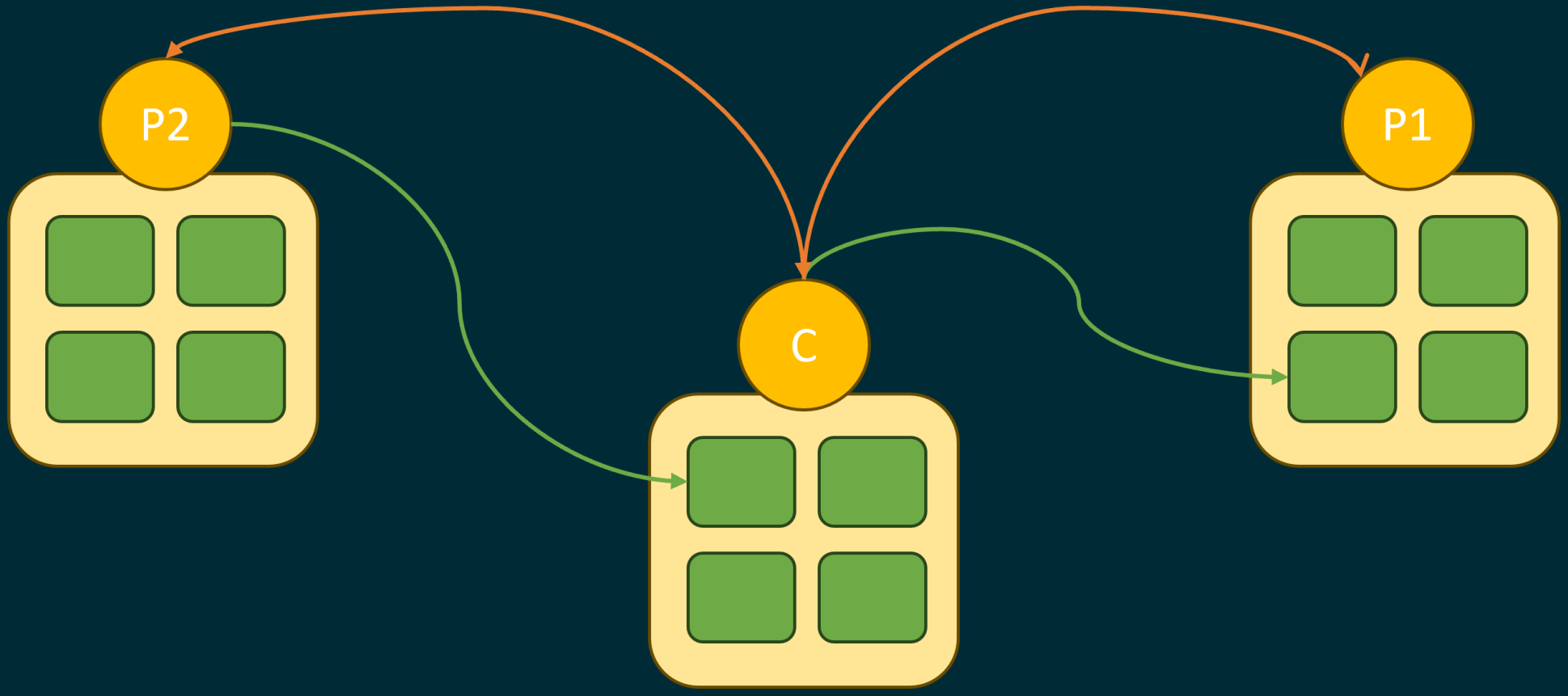
PODSTAWOWE KONFIGURACJE W NAGIOSIE



INNE

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


MySQL
WEB
Centreon
/etc/centreon-engine/*.cfg
Nagios


P2
P1
C

WSZYSTKO ZACZYNA SIĘ NA PAPIERZE

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

ANALIZA PRZYPADKU

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

~~SKY~~ SHELL IS THE LIMIT

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 LINUKSIE

```
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 LINUKSIE

```
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