Zabbix Conference Poland 2026

From Metrics to Meaning

Extending Zabbix with Flow Data and External Pipelines for Real-Time Network Intelligence

Prezentuje

Marcin Kaźmierczak

Czy ICMP i SNMP wystarczą do pełnej widoczności?

Gdzie szukasz przyczyny, gdy metryki są OK?

Czy widzisz ruch, który nie generuje alertów?

Co naprawdę wydarzyło się między dwoma pomiarami?

W jaki sposób Sycope może uzupełnić brakujące dane?

Jakie możliwości monitorowania daje NetFlow?

Jakie możliwości monitorowania daje NetFlow

- Monitorowanie całej sieci. Switche, routery, firewalle różnych producentów wysyłają NetFlow
- NetFlow to metadane o ruchu sieciowym – zbierane są tylko najważniejsze dane dla naszej analizy

Section	Variable	Value
Basic Fields		
1	Time	2022-11-29 17:02:00
2	Client IP	172.16.20.198
3	Server IP	216.58.215.110
4	IP Protocol	6
5	Protocol Name	TCP (6)
6	Client Port	55250
7	Server Port	443
8	Application	443
9	Application Name	https (443)
10	Exporter IPs	172.16.100.1
11	Interfaces	172.16.100.1[4],172.16.100.1[5
12	Client Function	Workstations

Client IP	172.16.20.198
Server IP	216.58.215.110

Kto?

IP Protocol	6
Protocol Name	TCP (6)
Client Port	55250
Server Port	443
Application	443
Application Name	https (443)

Co?

Exporter IPs	172.16.100.1
Interfaces	172.16.100.1[4],172.16.100.1[5]

Gdzie?

Jakie możliwości monitorowania daje NetFlow

- Nawet 80–90% problemów w sieci można zauważyć wcześniej, analizując sam przepływ ruchu
- Nie trzeba znać treści pakietów, wystarczy wiedzieć:
  - Kto wysyła
  - Dokąd wysyła
  - Jak dużo
  - Jak często

To właśnie pokazuje NetFlow.

Section	Variable	Value
Measures		
30	Active Time	30296
31	First Timestamp	2022-11-29 16:56:58
32	Last Timestamp	2022-11-29 16:57:53
33	Bytes	33.70KB
34	Client Bytes	22.57KB
35	Server Bytes	11.13KB
36	Bits	269,576
37	Client Bits	180,560
38	Server Bits	89,016
39	Bits/s	4.49kb/s
40	Clients Bits/s	3.01kb/s
41	Server Bits/s	1.48kb/s
42	Packets	124
43	Client Packets	54
44	Server Packets	70
45	Packets/s	16.53pkt/s
46	Client Packets/s	0.90pkt/s
47	Server Packets/s	1.17pkt/s
48	Flows	12

30	Active Time	30296
31	First Timestamp	2022-11-29 16:56:58
32	Last Timestamp	2022-11-29 16:57:53

Kiedy?

36	Bits	269,576
37	Client Bits	180,560
38	Server Bits	89,016
39	Bits/s	4.49kb/s
40	Clients Bits/s	3.01kb/s
41	Server Bits/s	1.48kb/s
42	Packets	124
43	Client Packets	54
44	Server Packets	70
45	Packets/s	16.53pkt/s
46	Client Packets/s	0.90pkt/s
47	Server Packets/s	1.17pkt/s
48	Flows	12

Jak dużo?

Sycope + Zabbix

Pasywne monitorowanie NetFlow uzupełnia luki aktywnego monitoringu ICMP/SNMP

AKTYWNE MONITOROWANIE
ICMP / SNMP w ZABBIX

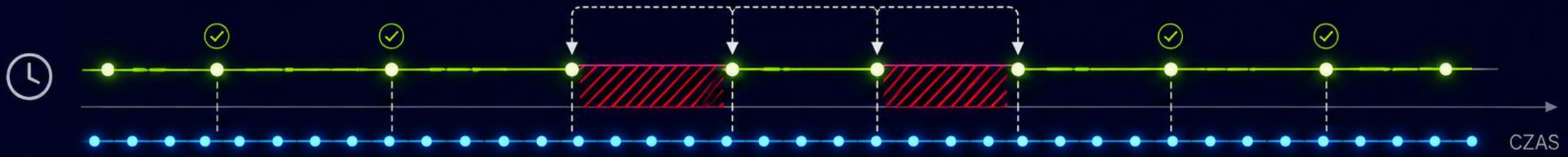
- Widoczność tylko w momentach sondowania

LUKI W AKTYWNYM MONITORINGU

Problemy mogą wystąpić między sondowaniami i pozostać niewykryte

PASYWNE MONITOROWANIE
NETFLOW w SYCOPE

- Ciągła widoczność – 24/7/365



RAZEM = PEŁNY OBRAZ SIECI

ZABBIX
Dane o urządzeniach, alertach, dostępności

API

Integracja przez API

SYCOPE
Dane o ruchu, rozmowach, aplikacjach, top talkers

- Więcej kontekstu
- Szybsza identyfikacja problemów
- Lepsze decyzje
- Optymalizacja sieci
- Oszczędność czasu i zasobów

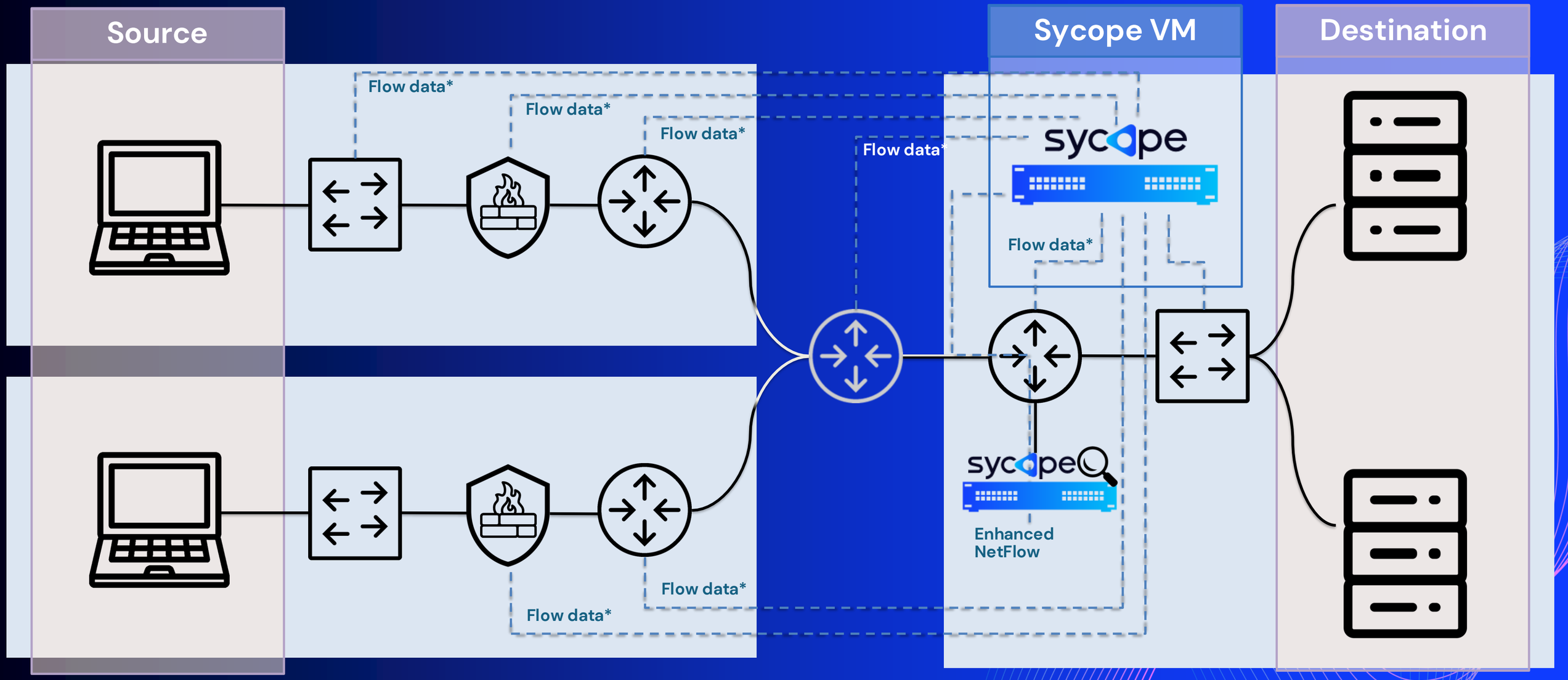
Monitoruj swoją sieć w czasie rzeczywistym – za darmo!

- Bez konieczności podawania karty płatniczej
- Gotowe do użycia od razu po instalacji
- Wykrywanie zagrożeń i anomalii
- Do 5 000 flows/s
- Retencja danych ograniczona do 14 dni

https://free.sycope.com

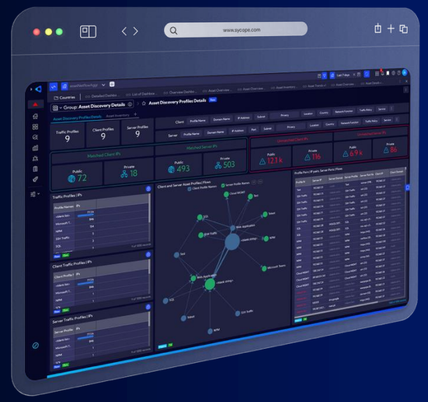
Jak działa Sycope?

Wiele źródeł ruchu – jedno centrum dowodzenia

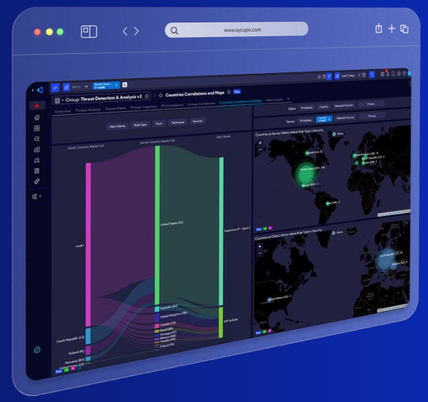


Platforma Network Observability

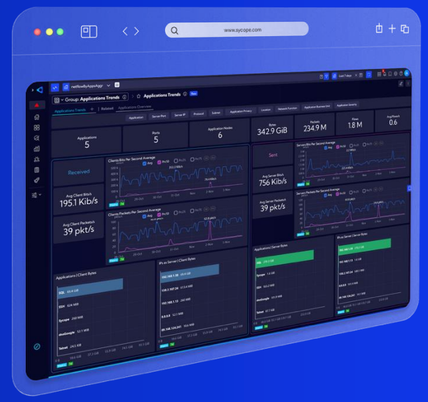
Podstawą systemu jest Visibility, zasilany danymi NetFlow, dostarczający informacje o ruchu sieciowym. Kolejne moduły wzbogacają informacje o ruchu sieciowym, o wskaźniki wydajnościowe, analizę L7, wykrywanie anomalii i inwentaryzację urządzeń.



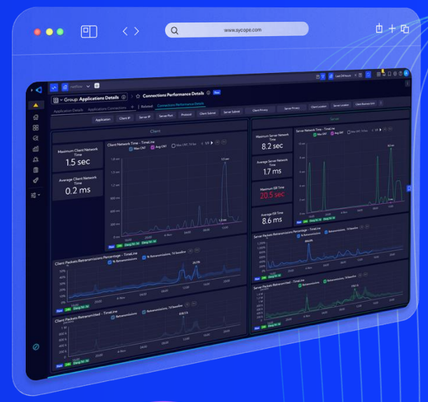
VISIBILITY
Analiza ruchu



PERFORMANCE
Wydajność sieci (NPM)



SECURITY
Wykrywanie zagrożeń



ASSET DISCOVERY
Inwentaryzacja zasobów

Mądrzejsze decyzje z Sycope

NETWORK INTELLIGENCE

ZESPÓŁ NOC

ZESPÓŁ SOC

NTA

Network Traffic Analysis

- Inteligentne trendy & Baselines
- Pasywna analiza ruchu flowego

NPM

Network Performance Monitor

- Automatyczna inwentaryzacja zasobów
- Wykrywanie aplikacji
- Bez dodatkowych uprawnień

sycope

UNIFIED PLATFORM

NOC + SOC
w jednym widoku

SHARED CONTEXT

NDR

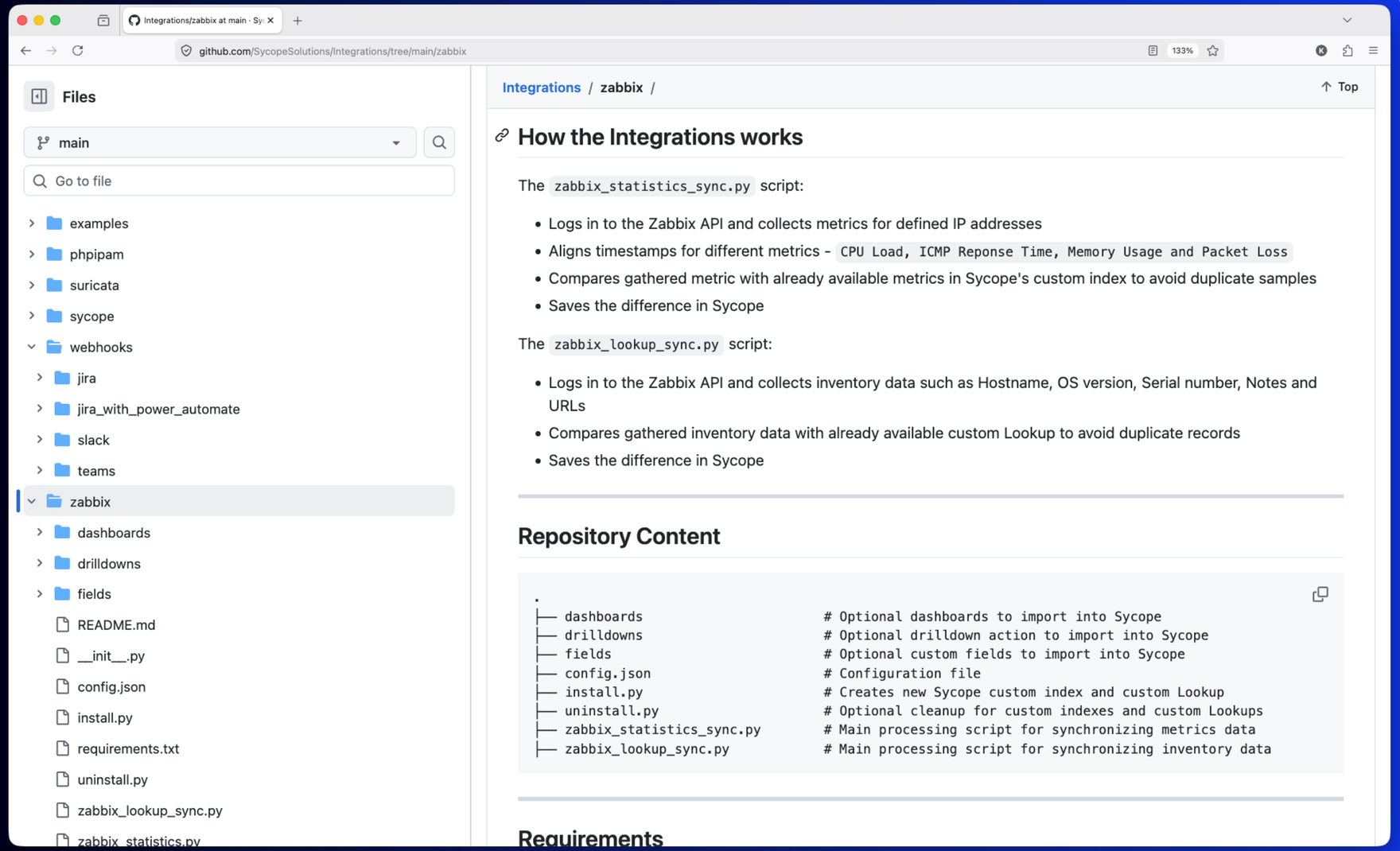
Network Detection and Response

- Ponad 70 reguł i alertów
- Repozytorium online — CTI
- IDS oraz analiza pakietów

Integracje

SycopeSolutions – Otwarte Repozytorium GitHub

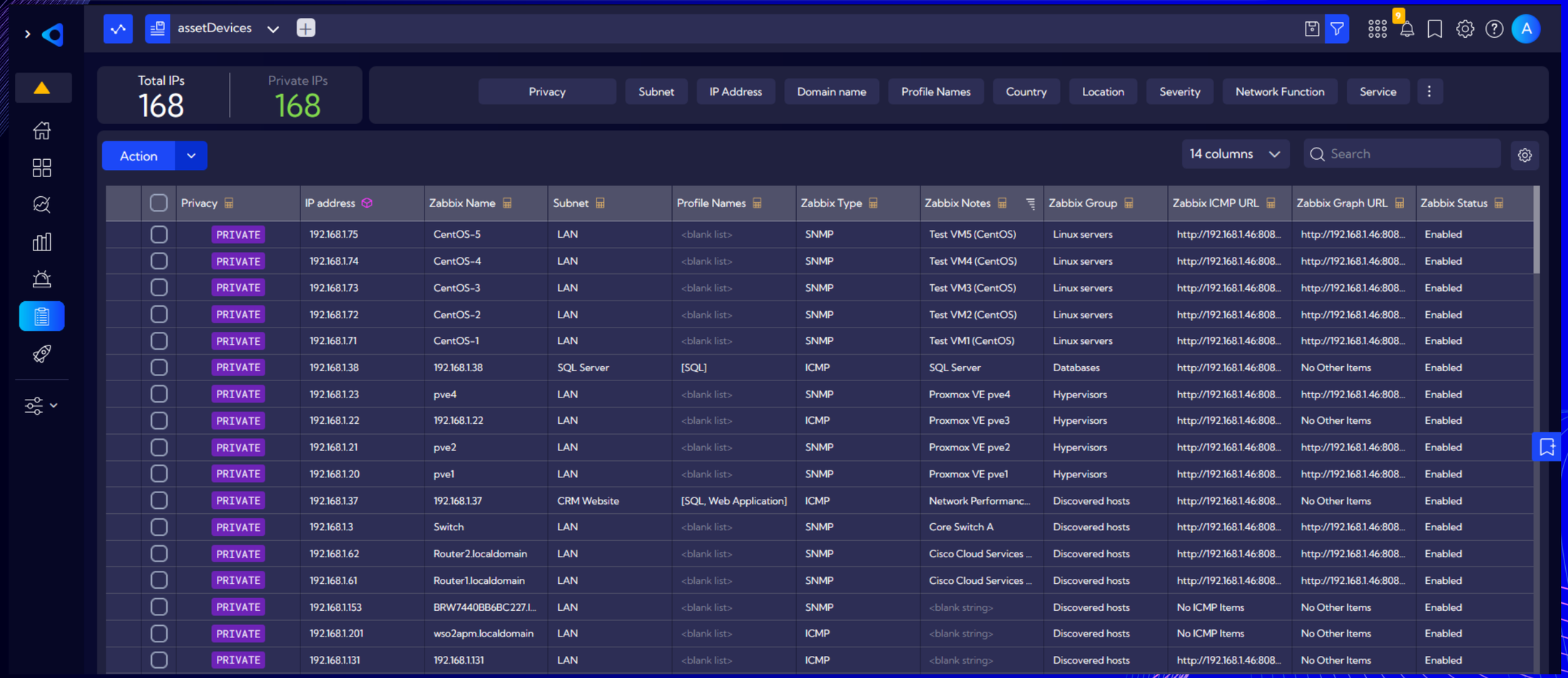
- https://github.com/SycopeSolutions/



Łączenie danych – wspólne GUI

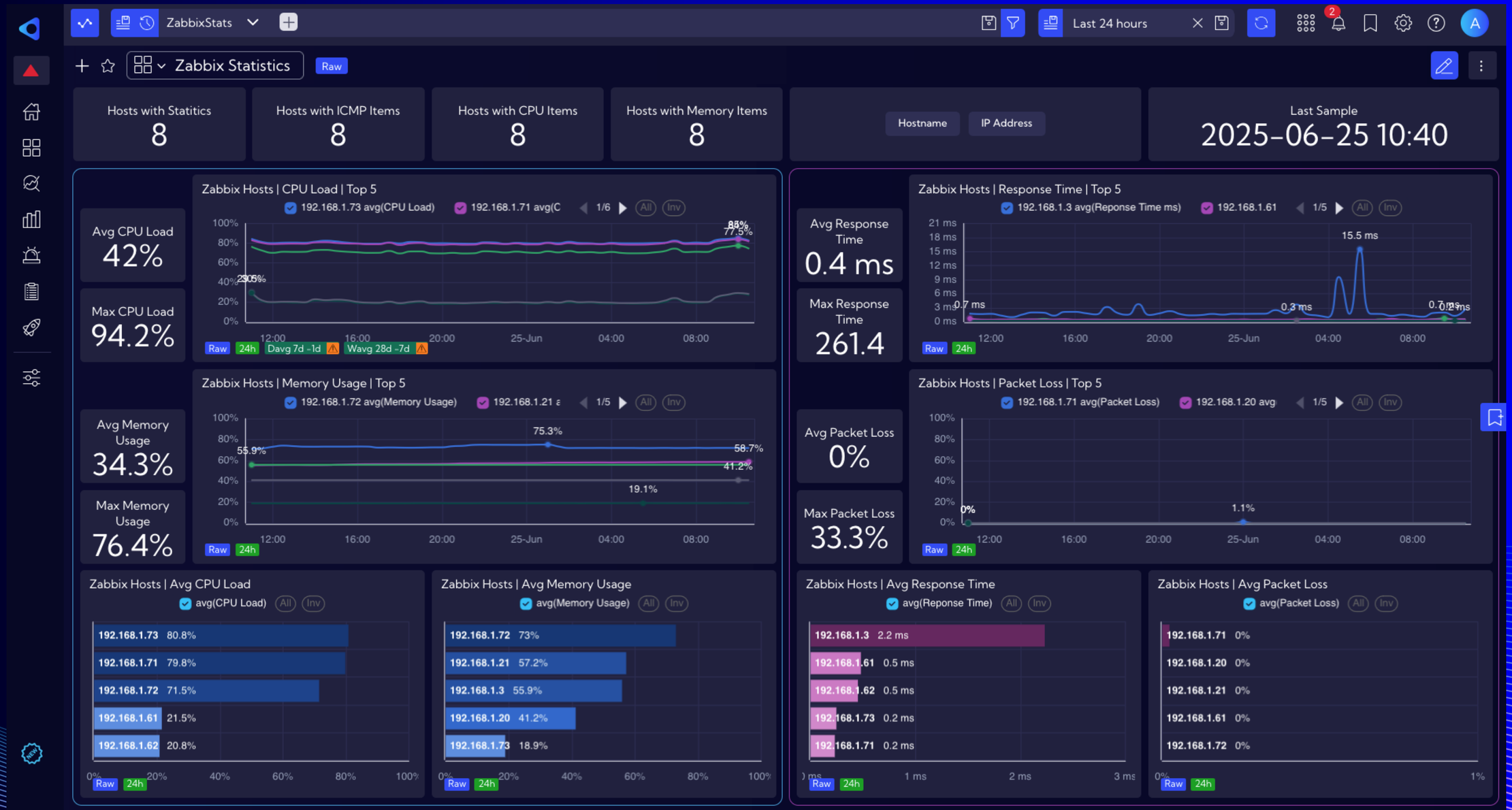
Synchronizacja Inwentaryzacji

- Zidentyfikuj, które Hosty są Włączone i jakie Elementy Zabbix są dostępne
- Używaj filtrów w Sycope na podstawie Inwentarza Zabbix (dane z SNMP, WMI, SSH)



Privacy	IP address	Zabbix Name	Subnet	Profile Names	Zabbix Type	Zabbix Notes	Zabbix Group	Zabbix ICMP URL	Zabbix Graph URL	Zabbix Status
PRIVATE	192.168.1.75	CentOS-5	LAN	<blank list>	SNMP	Test VM5 (CentOS)	Linux servers	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
PRIVATE	192.168.1.74	CentOS-4	LAN	<blank list>	SNMP	Test VM4 (CentOS)	Linux servers	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
PRIVATE	192.168.1.73	CentOS-3	LAN	<blank list>	SNMP	Test VM3 (CentOS)	Linux servers	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
PRIVATE	192.168.1.72	CentOS-2	LAN	<blank list>	SNMP	Test VM2 (CentOS)	Linux servers	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
PRIVATE	192.168.1.71	CentOS-1	LAN	<blank list>	SNMP	Test VM1 (CentOS)	Linux servers	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
PRIVATE	192.168.1.38	192.168.1.38	SQL Server	[SQL]	ICMP	SQL Server	Databases	http://192.168.1.46:808...	No Other Items	Enabled
PRIVATE	192.168.1.23	pve4	LAN	<blank list>	SNMP	Proxmox VE pve4	Hypervisors	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
PRIVATE	192.168.1.22	192.168.1.22	LAN	<blank list>	ICMP	Proxmox VE pve3	Hypervisors	http://192.168.1.46:808...	No Other Items	Enabled
PRIVATE	192.168.1.21	pve2	LAN	<blank list>	SNMP	Proxmox VE pve2	Hypervisors	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
PRIVATE	192.168.1.20	pve1	LAN	<blank list>	SNMP	Proxmox VE pve1	Hypervisors	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
PRIVATE	192.168.1.37	192.168.1.37	CRM Website	[SQL, Web Application]	ICMP	Network Performanc...	Discovered hosts	http://192.168.1.46:808...	No Other Items	Enabled
PRIVATE	192.168.1.3	Switch	LAN	<blank list>	SNMP	Core Switch A	Discovered hosts	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
PRIVATE	192.168.1.62	Router2.localdomain	LAN	<blank list>	SNMP	Cisco Cloud Services ...	Discovered hosts	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
PRIVATE	192.168.1.61	Router1.localdomain	LAN	<blank list>	SNMP	Cisco Cloud Services ...	Discovered hosts	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
PRIVATE	192.168.1.153	BRW7440BB6BC227.l...	LAN	<blank list>	SNMP	<blank string>	Discovered hosts	No ICMP Items	No Other Items	Enabled
PRIVATE	192.168.1.201	wso2apm.localdomain	LAN	<blank list>	ICMP	<blank string>	Discovered hosts	No ICMP Items	No Other Items	Enabled
PRIVATE	192.168.1.131	192.168.1.131	LAN	<blank list>	ICMP	<blank string>	Discovered hosts	http://192.168.1.46:808...	No Other Items	Enabled

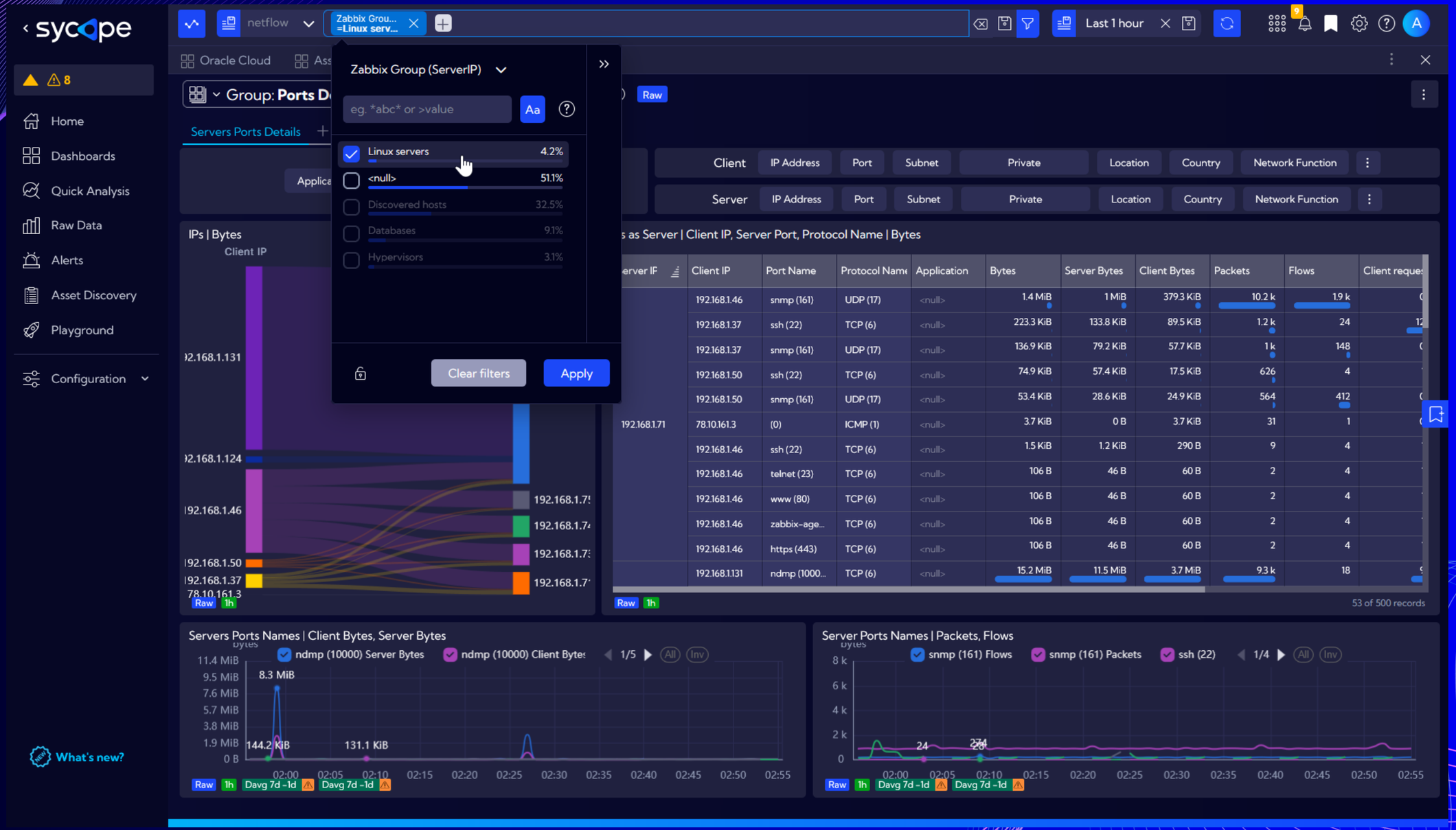
Zabbix Statistics Dashboard



Zabbix Inventory Dashboard

IP address	Zabbix Name	Zabbix Type	Zabbix Status	Zabbix Group	Zabbix Notes	Zabbix OS	Zabbix Serial No	Zabbix ICMP URL	Zabbix Graph URL
192.168.1.75	CentOS-5	SNMP	Enabled	Linux servers	Test VM5 (CentOS)	<blank string>	<blank string>	http://192.168.1.46:808	http://192.168.1.46:808
192.168.1.74	CentOS-4	SNMP	Enabled	Linux servers	Test VM4 (CentOS)	<blank string>	<blank string>	http://192.168.1.46:808	http://192.168.1.46:808
192.168.1.73	CentOS-3	SNMP	Enabled	Linux servers	Test VM3 (CentOS)	<blank string>	<blank string>	http://192.168.1.46:808	http://192.168.1.46:808
192.168.1.72	CentOS-2	SNMP	Enabled	Linux servers	Test VM2 (CentOS)	<blank string>	<blank string>	http://192.168.1.46:808	http://192.168.1.46:808
192.168.1.71	CentOS-1	SNMP	Enabled	Linux servers	Test VM1 (CentOS)	<blank string>	<blank string>	http://192.168.1.46:808	http://192.168.1.46:808
192.168.1.38	192.168.1.38	SNMP	Enabled	Databases	SQL Server	<blank string>	<blank string>	http://192.168.1.46:808	No Other Items
192.168.1.23	pve4	SNMP	Enabled	Hypervisors	Proxmox VE pve4	<blank string>	<blank string>	http://192.168.1.46:808	http://192.168.1.46:808
192.168.1.22	192.168.1.22	SNMP	Enabled	Hypervisors	Proxmox VE pve3	<blank string>	<blank string>	http://192.168.1.46:808	No Other Items
192.168.1.21	pve2	SNMP	Enabled	Hypervisors	Proxmox VE pve2	<blank string>	<blank string>	http://192.168.1.46:808	http://192.168.1.46:808
192.168.1.20	pve1	SNMP	Enabled	Hypervisors	Proxmox VE pve1	<blank string>	<blank string>	http://192.168.1.46:808	http://192.168.1.46:808
192.168.1.37	192.168.1.37	SNMP	Enabled	Discovered hosts	Network Performance Monitor	<blank string>	<blank string>	http://192.168.1.46:808	No Other Items
192.168.1.3	Switch	SNMP	Enabled	Discovered hosts	Core Switch A	15.0(2)SE11	<blank string>	http://192.168.1.46:808	http://192.168.1.46:808
192.168.1.61	Router1.localdomain	SNMP	Enabled	Discovered hosts	Cisco Cloud Services Router 1000v	17.3.3	9EIACJ3VXDX	http://192.168.1.46:808	http://192.168.1.46:808
192.168.1.62	Router2.localdomain	SNMP	Enabled	Discovered hosts	Cisco Cloud Services Router 1000v	17.3.3	964R4WIWQY2	http://192.168.1.46:808	http://192.168.1.46:808
192.168.1.1	unifi.localdomain	SNMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	No ICMP Items	No Other Items
192.168.1.10	192.168.1.10	SNMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	No ICMP Items	No Other Items
192.168.1.11	192.168.1.11	ICMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	No ICMP Items	No Other Items
192.168.1.13	192.168.1.13	SNMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	http://192.168.1.46:808	No Other Items
192.168.1.14	192.168.1.14	SNMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	http://192.168.1.46:808	No Other Items
192.168.1.15	192.168.1.15	SNMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	http://192.168.1.46:808	No Other Items
192.168.1.16	192.168.1.16	ICMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	http://192.168.1.46:808	No Other Items
192.168.1.19	192.168.1.19	SNMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	http://192.168.1.46:808	No Other Items
192.168.1.27	192.168.1.27	ICMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	No ICMP Items	No Other Items
192.168.1.28	192.168.1.28	ICMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	No ICMP Items	No Other Items

Filtruj dowolny widok używając Fields i Inventory z Zabbix



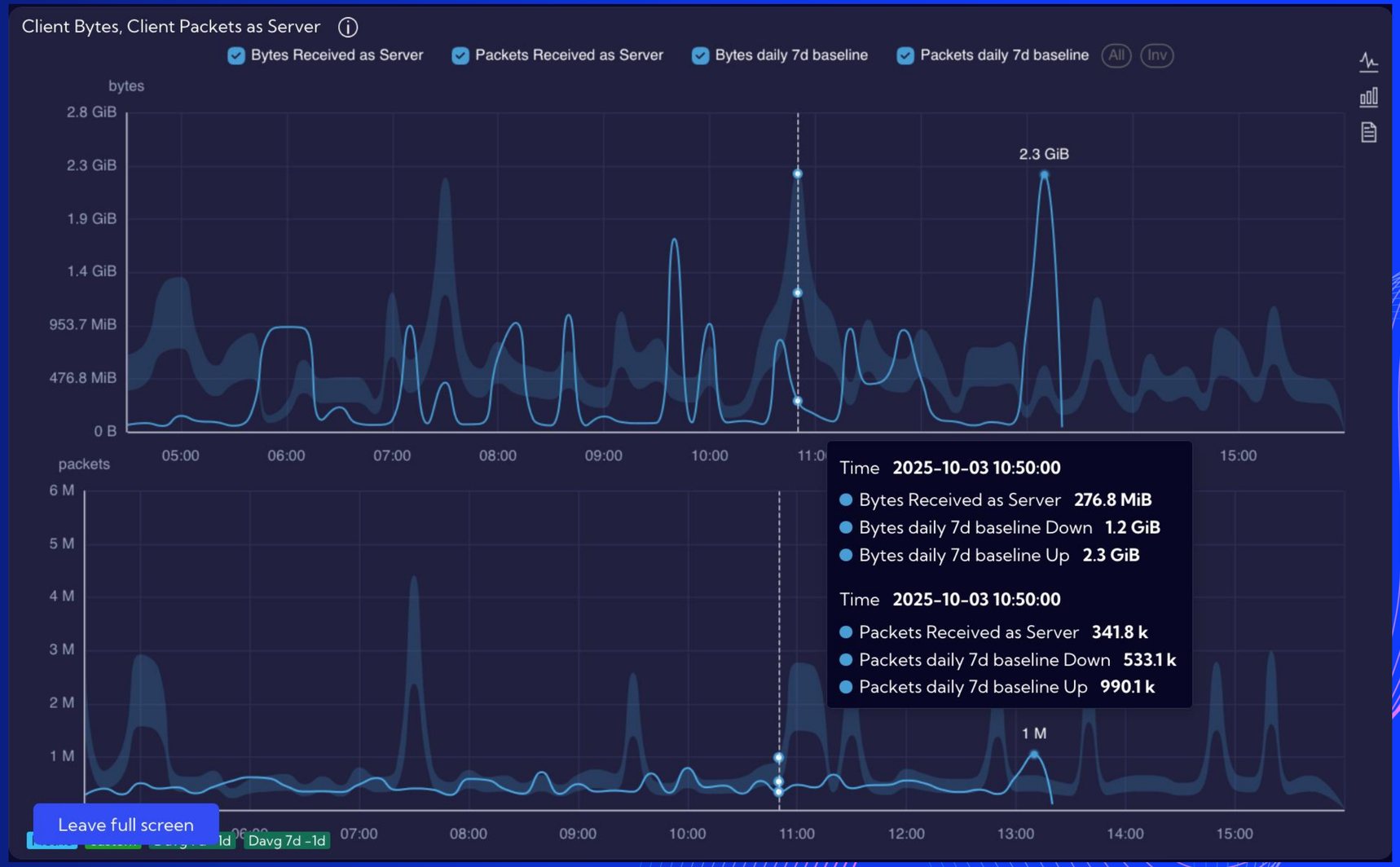
Automatyczne Trendy i Baseline

Efekt wstążki dla bieżącego i przyszłego ruchu

Zakres dla baseline – wartości Górna i Dolna

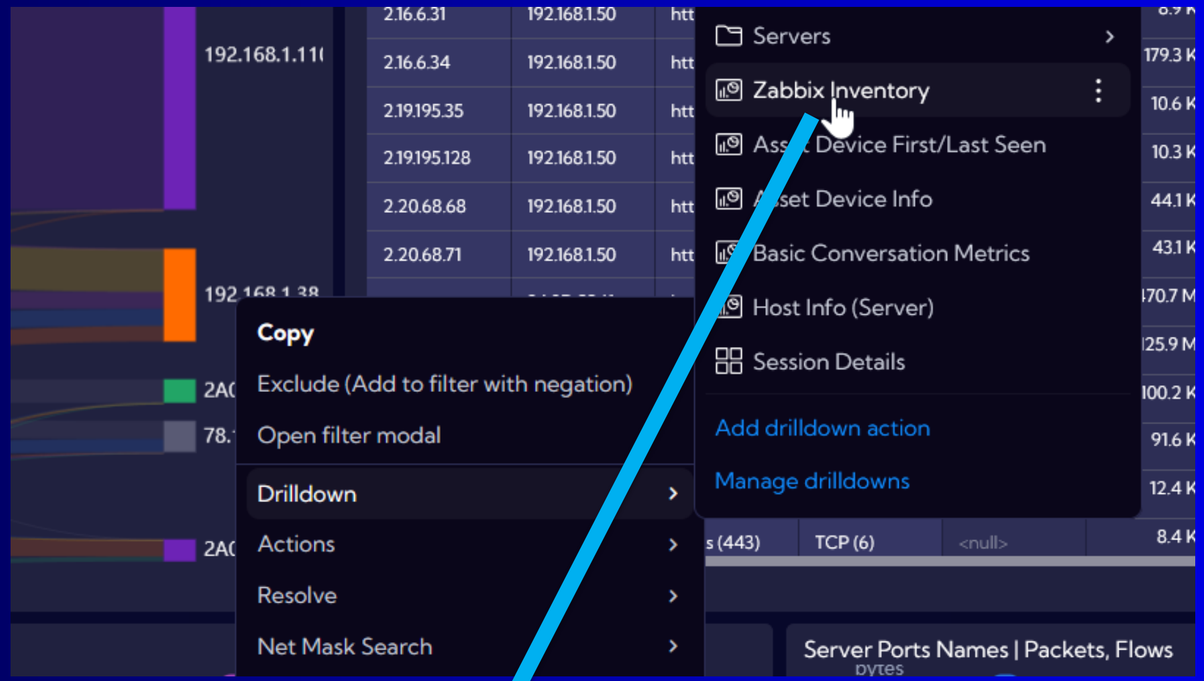
Twórz trendy na dowolnym wykresie używając wszystkich dostępnych metryk

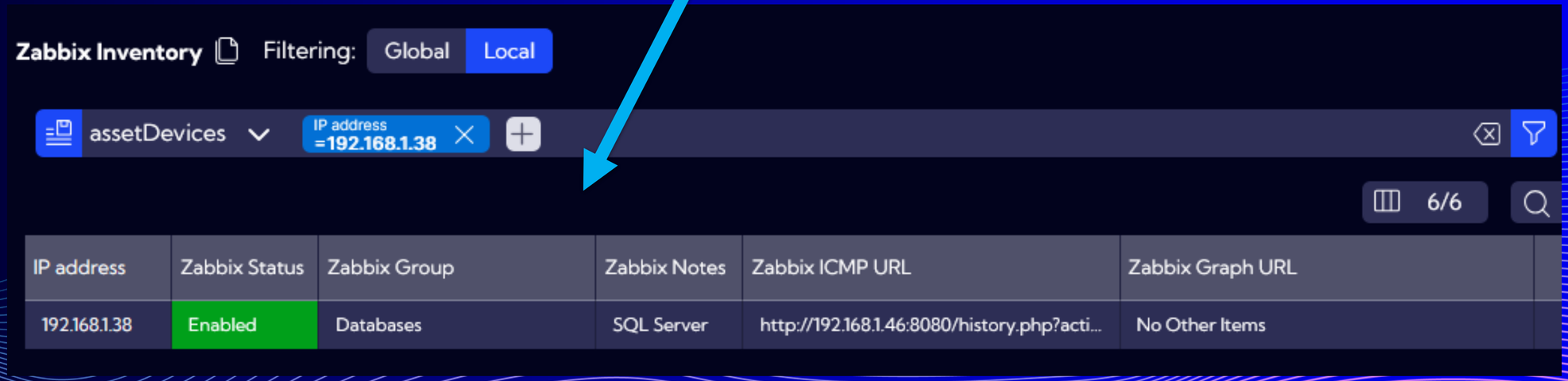
Wsparcie dla punktów końcowych, aplikacji, podsieci, lokalizacji, krajów, AS



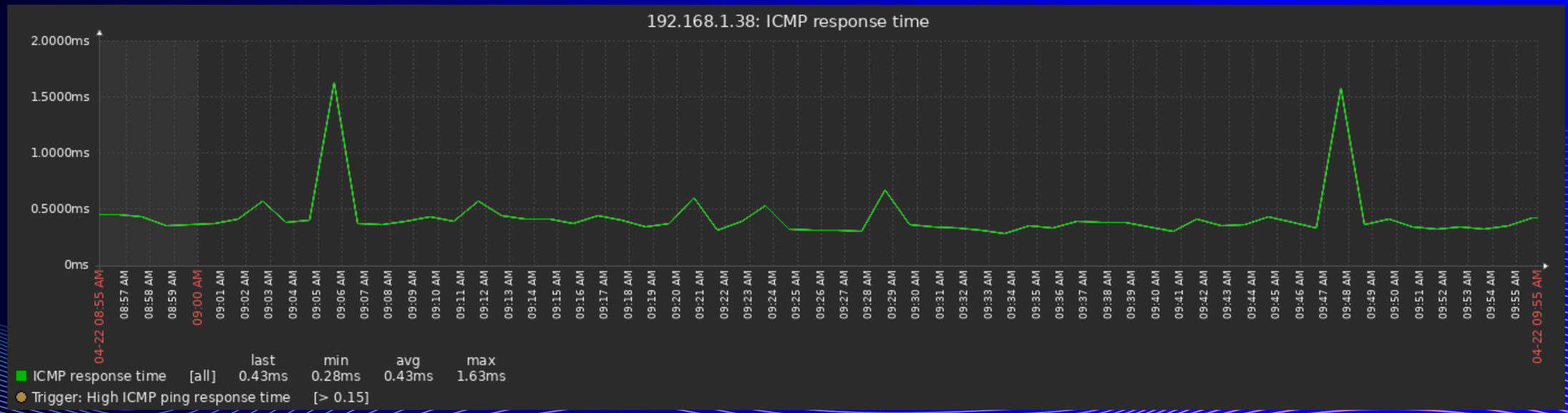
Przejdźmy do Zabbixa...

Akcje Drilldown, aby wyświetlić dowolne dane z Zabbix i...





...przejdź bezpośrednio do dashboardów Zabbix



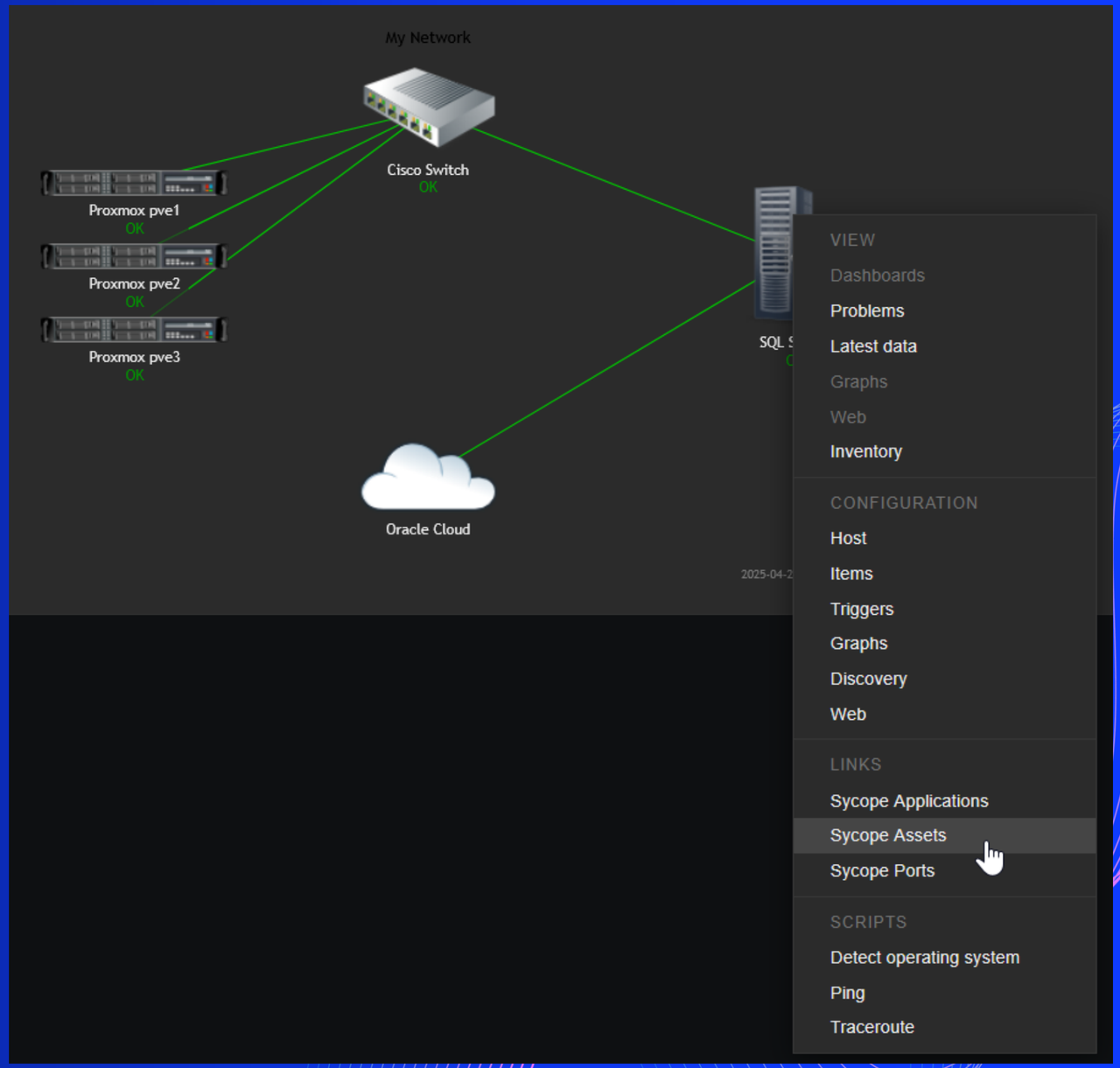
Możliwość umieszczenia czegokolwiek na Mapie

Dodaj adresy URL Sycope do dowolnych wbudowanych lub niestandardowych dashboardów (+definiuj automatyczny filtr dla adresu IP lub innej wartości)

- Wiele hiperłączy do każdego modułu Sycope

Używaj Szablonów Zabbix do prezentacji (etykiety z makrami):

- Licznik alertów
- Serwery z dostępem do Internetu
  - Publiczne połączenia „od" i „do" Hosta
- Liczba połączeń, sesji
- Otwarte porty



Host	Name ▲	Last check	Last value	Change	Tags	Info
192.168.1.50	Asset Discovery - Active Services (count)	4m 58s	7		component: asset_di…	Graph
192.168.1.50	Asset Discovery - Active Services (port list)	4m 57s	22 (not defined), 23 (…		component: asset_di…	History
192.168.1.50	Asset Discovery - Matched Client Private IPs	4m 39s	1			
192.168.1.50	Asset Discovery - Matched Client Public IPs	4m 38s	0		component: asset_di…	Graph
192.168.1.50	Asset Discovery - Matched Server Private IPs	4m 37s	1		component: asset_di…	Graph
192.168.1.50	Asset Discovery - Matched Server Public IPs	4m 36s	0		component: asset_di…	Graph
192.168.1.50	Asset Discovery - Private Connections From Node	4m 43s	12		component: asset_di…	Graph
192.168.1.50	Asset Discovery - Private Connections To Node	4m 43s	5	-1	component: asset_di…	Graph
192.168.1.50	Asset Discovery - Public Connections From Node	4m 41s	102	-1	component: asset_di…	Graph
192.168.1.50	Asset Discovery - Public Connections To Node	4m 41s	0		component: asset_di…	Graph
192.168.1.50	Asset Discovery - Unmatched Client Private IPs	4m 34s	5		component: asset_di…	Graph
192.168.1.50	Asset Discovery - Unmatched Client Public IPs	4m 33s	0		component: asset_di…	Graph
192.168.1.50	Asset Discovery - Unmatched Server Private IPs	4m 33s	1		component: asset_di…	Graph
192.168.1.50	Asset Discovery - Unmatched Server Public IPs	4m 32s	0		component: asset_di…	Graph
192.168.1.50	Performance - High Client Network Latency	4m 56s	0		component: performa…	Graph
192.168.1.50	Performance - High Client Network Latency (detail)	4m 50s	Total: 0, Acknowledge…		component: performa…	History
192.168.1.50	Performance - High Server Network Latency	4m 55s	0		component: performa…	Graph
192.168.1.50	Performance - High Server Network Latency (detail)	4m 48s	Total: 0, Acknowledge…		component: performa…	History
192.168.1.50	Security - Horizontal Scan	4m 53s	0		component: security	Graph
192.168.1.50	Security - Horizontal Scan (detail)	4m 48s	Total: 0, Acknowledge…		component: security	History
192.168.1.50	Security - Vertical Scan	4m 51s	0		component: security	Graph
192.168.1.50	Security - Vertical Scan (detail)	4m 45s	Total: 0, Acknowledge…		component: security	History
192.168.1.50	Visibility - Initial connections from Public IPs	4m 53s	0		component: visibility	Graph
192.168.1.50	Visibility - Initial connections from Public IPs (detail)	4m 47s	Total: 0, Acknowledge…		component: visibility	History
192.168.1.50	Visibility - Only SYN Client TCP Flag	4m 51s	8	+2	component: visibility	Graph
192.168.1.50	Visibility - Only SYN Client TCP Flag (detail)	4m 45s	Total: 8, Acknowledge…		component: visibility	History

22 (not defined), 23 (not defined), 80 (not defined), 443 (not defined), 2055 (NETFLOW), 2055 (not defined), 10050 (not defined)

Displaying 26 of 26 found

Sycope Monitoring

All dashboards / Sycope Monitoring

Edit dashboard | Zoom out | 2026-04-28 10:30:04 – now

SYN TCP Flag

8.00

Visibility - Only SYN Client …

Public Init Conns

0.00

Visibility - Initial connections from Publi…

Horizontal Scan

0.00

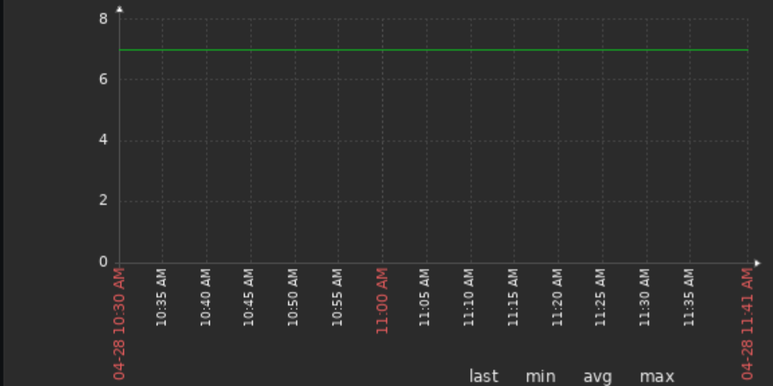
Security - Horizontal Scan

Vertical Scan

0.00

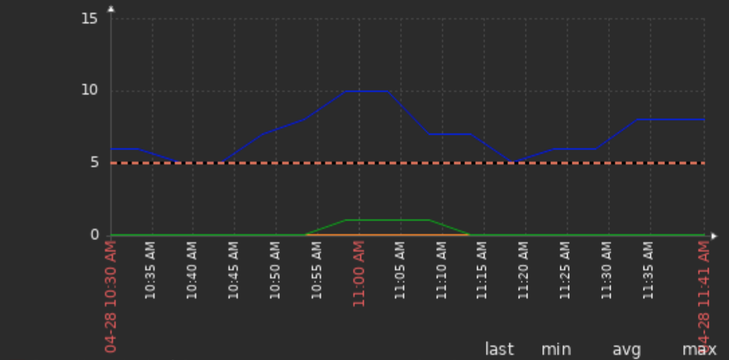
Security - Vertical Scan

Active Services



		last	min	avg	max
Asset Discovery - Active Services (count)	[avg]	7	7	7	7

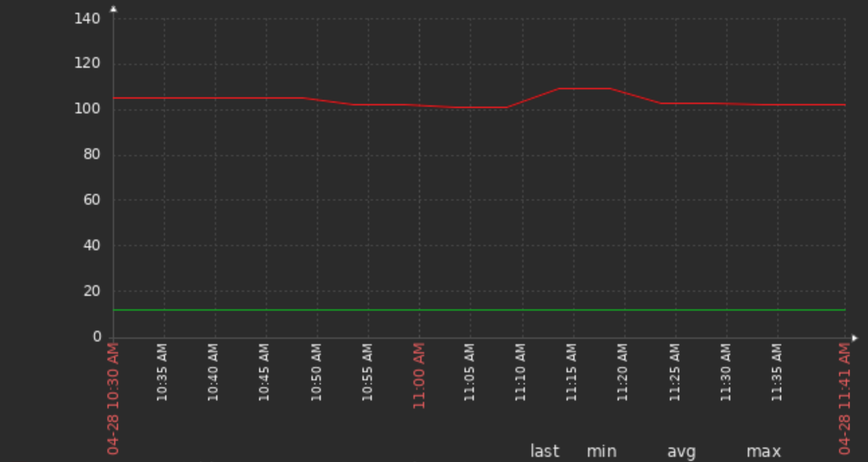
Security Alerts



		last	min	avg	max
Security - Vertical Scan	[avg]	0	0	0	0
Visibility - Only SYN Client TCP Flag	[avg]	8	5	7	10
Visibility - Initial connections from Public IPs	[avg]	0	0	0	0
Security - Horizontal Scan	[avg]	0	0	0.2143	1

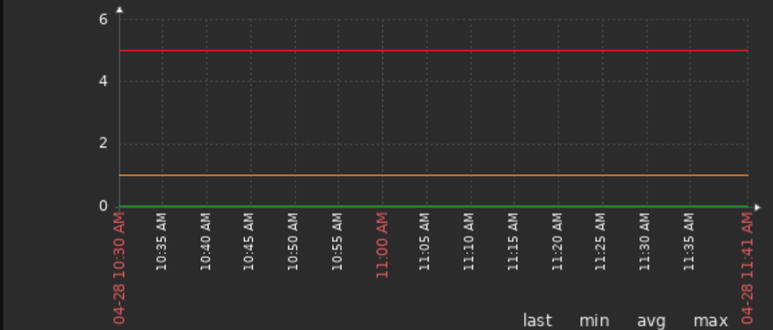
Trigger: Sycope: Vertical scan HIGH on 192.168.1.50	[> 5]
Trigger: Sycope: Only SYN TCP Flag alerts HIGH on 192.168.1.50	[> 5]
Trigger: Sycope: Initial connections from public IPs HIGH on 192.168.1.50	[> 5]

Connections From Node



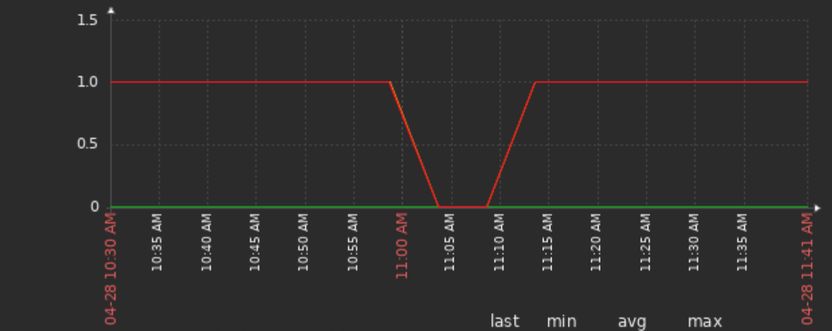
		last	min	avg	max
Asset Discovery - Public Connections From Node	[avg]	102	101	103.6667	109
Asset Discovery - Private Connections From Node	[avg]	12	12	12	12

Unmatched IPs



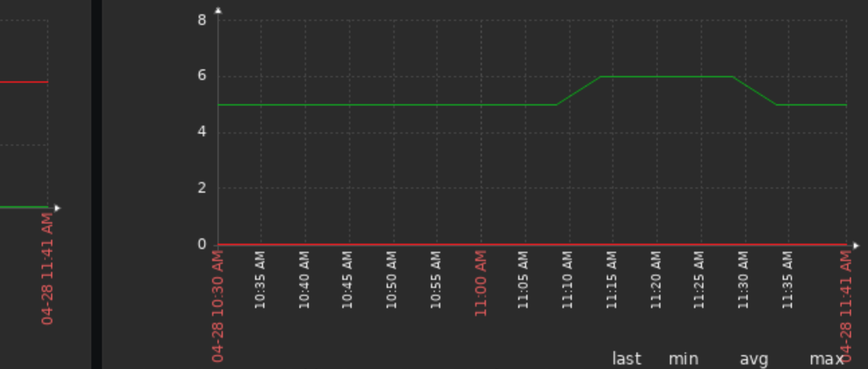
		last	min	avg	max
Asset Discovery - Unmatched Server Public IPs	[avg]	0	0	0	0
Asset Discovery - Unmatched Server Private IPs	[avg]	1	1	1	1
Asset Discovery - Unmatched Client Public IPs	[avg]	0	0	0	0
Asset Discovery - Unmatched Client Private IPs	[avg]	5	5	5	5

Matched IPs



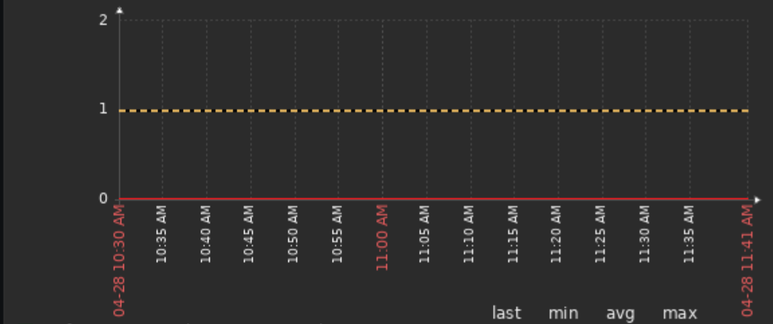
		last	min	avg	max
Asset Discovery - Matched Server Public IPs	[avg]	0	0	0	0
Asset Discovery - Matched Server Private IPs	[avg]	1	0	0.8333	1
Asset Discovery - Matched Client Public IPs	[avg]	0	0	0	0
Asset Discovery - Matched Client Private IPs	[avg]	1	0	0.8333	1

Connections To Node



		last	min	avg	max
Asset Discovery - Public Connections To Node	[avg]	0	0	0	0
Asset Discovery - Private Connections To Node	[avg]	5	5	5.3333	6

Performance Alerts



		last	min	avg	max
Performance - High Server Network Latency	[avg]	0	0	0	0
Performance - High Client Network Latency	[avg]	0	0	0	0

Co zrobić, gdy coś się wydarzy?

Co zrobić, gdy coś się wydarzy? (szablon dla Zabbixa)

Time ▾	Severity	Recovery time	Status	Info	Host	Problem	Duration	Update	Actions	Tags
11:18:22 AM	Warning		PROBLEM		192.168.1.50	Sycope: Only SYN TCP Flag alerts detected on 192.168.1.50	1m 11s	Update		component: visibility
11:00										
10:48:22 AM	High	11:18:22 AM	RESOLVED		192.168.1.50	Sycope: Only SYN TCP Flag alerts HIGH on 192.168.1.50	30m	Update		component: visibility

Displaying 2 of 2 found

Host availability

10	2	0	39	51
Available	Not available	Mixed	Unknown	Total

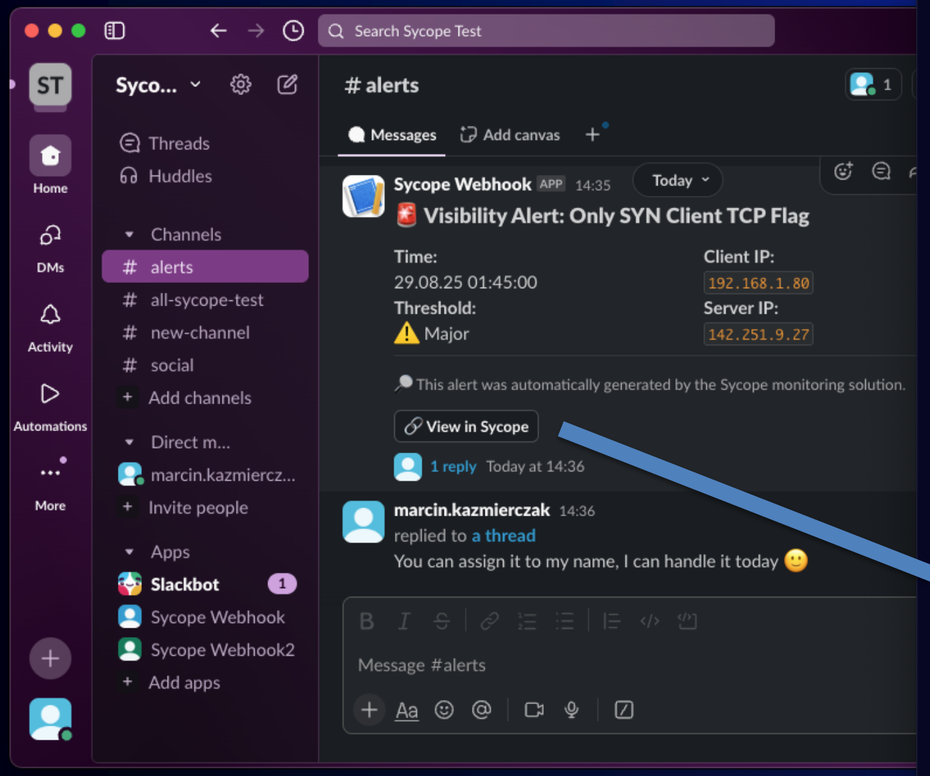
Problems by severity

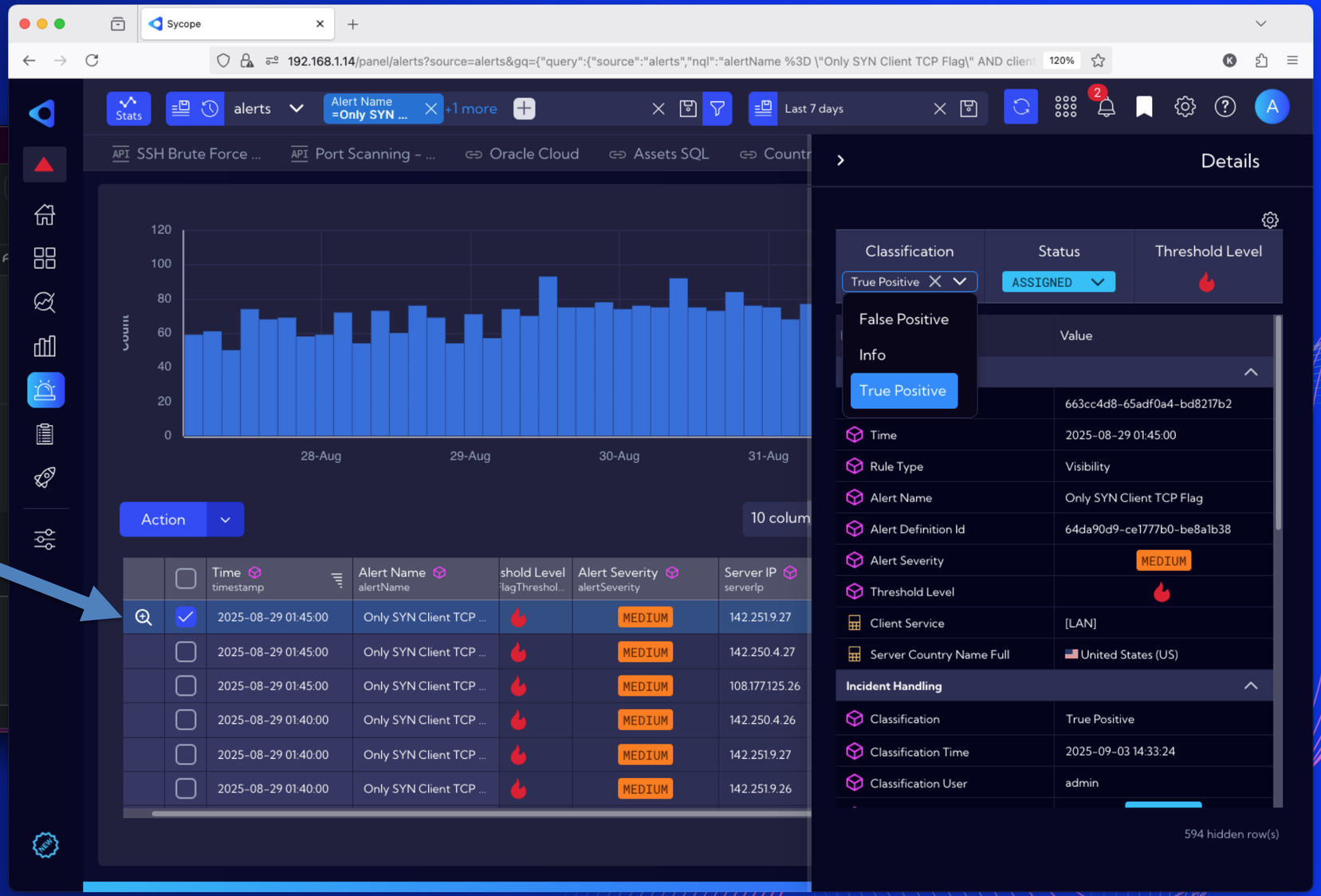
0	21	10	23	3	0
Disaster	High	Average	Warning	Information	Not classified

Current problems

Time ▾	Info	Host	Problem • Severity	Duration	Update	Actions	Tags
11:23:41 AM		Samsung.localdomain	Sycope: Only SYN TCP Flag alerts detected on Samsung.localdomain	3m 53s	Update		component: visibility
11:23:23 AM		192.168.1.50	Sycope: Only SYN TCP Flag alerts HIGH on 192.168.1.50	4m 11s	Update		component: visibility
11:23:14 AM		192.168.1.29	Sycope: Horizontal scan HIGH on 192.168.1.29	4m 20s	Update		component: security
11:00							

Co zrobić, gdy coś się wydarzy? (przykład Slack)





Więcej sposobów integracji

Wysyłanie Syslog lub SNMP Trapów przy użyciu Reguł i wyzwolonych Alertów (Wydajność, Widoczność, Odkrywanie Zasobów, Bezpieczeństwo)

Automatyczne Akcje REST API w Alertach lub ad hoc Drilldown

- Zmiana statusu Hosta między Wyłączony a Włączony
- Tworzenie Okresów Konserwacji dla hostów

Pytaj Sycope o cokolwiek przez REST API (użyj widgetów jako przykładu)

Niestandardowy Szablon Zabbix – przykład wyniku dla jednego Hosta:

- Bezpieczeństwo – Skanowanie Horyzontalne (alert):
  - Łącznie 10 (wyzwolonych alertów)
  - Potwierdzonych: 1, Fałszywie Pozytywnych: 0
- Aktywne Usługi:
  - 137 (NETBIOS), 445 (SMB), 1433 (SQL), 3389 (RDP)
- Niedopasowane Prywatne IP Klientów: 1
- Publiczne Połączenia Od Węzła: 73
- Publiczne Połączenia Do Węzła: 0

Modyfikuj dowolną zdefiniowaną Podsieć lub pojedyncze IP przez API (Zabbix, DHCP itp.)

Dodawaj odkryte adresy IP przez Sycope do Zabbix

Monitoruj swoją sieć w czasie rzeczywistym – za darmo!

- Bez konieczności podawania karty płatniczej
- Gotowe do użycia od razu po instalacji
- Wykrywanie zagrożeń i anomalii
- Do 5 000 flows/s
- Retencja danych ograniczona do 14 dni

https://free.sycope.com

Dziękuję!