Zarządzanie sieciowymi systemami wykrywania włamań

Borys Uchański

Plan prezentacji

- Wykrywanie włamań
- System Snort
- Zarządzanie wykrywaniem włamań
- Implementacja
- Intusion Detection Message Exchange Format

Włamanie

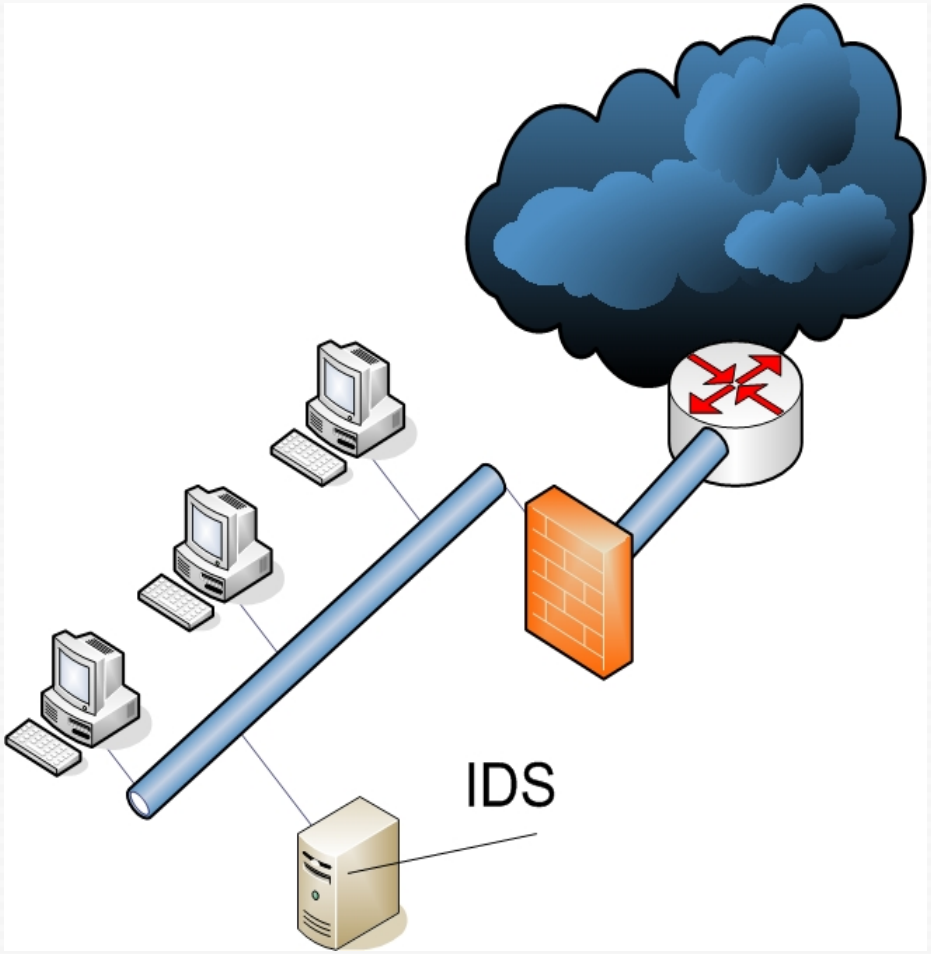
- *“Włamanie to nieautoryzowany dostęp do sieci lub systemu podłączonego do sieci, czyli celowe lub przypadkowe uzyskanie dostępu do systemu informacyjnego, włączając złośliwe działanie przeciwko temu systemowi lub nieautoryzowane użycie zasobów tego systemu.“*

  ISO/IEC Committee Draft 18043, Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems

- Podstawowa klasyfikacja:
  - zbieranie informacji
  - odmowa usługi
  - penetracja

Sieciowe systemy wykrywania włamań

- Analiza ruchu sieciowego w czasie rzeczywistym
- Dekodowanie protokołów
- Wykrywanie wzorców
- Wykrywanie anomalii
- Reakcja



Wykrywanie wzorców

- Wykrywanie znanych ataków na podstawie ich charakterystycznych cech
- Dopasowywanie wzorców (sygnatur, reguł) do monitorowanego ruchu sieciowego
- Sygnatury tworzone na podstawie rzeczywistych, zaobserowanych ataków
- Sygnatury darmowe lub od komercyjnych dostawców

Wykrywanie wzorców - przykład

- Hipotetyczny atak polegający na przepełnieniu bufora zbyt długim argumentem komendy PASS
- `alert tcp $EXTERNAL_NET any -> 192.168.1.2 21 (msg:"FTP przepelnienie bufora argumentem PASS"; flow:to_server,established; content:"PASS"; nocase; isdataat:100,relative; content:!“|0a|“; distance:0; within: 100; reference:bugtraq,777777; classtype:attempted-admin; sid:123123; rev:7;)`

Wykrywanie anomalii

- Założenie: normalne zachowanie da się zparametryzować
- Wykrywanie ataków przez porównywanie obserwowanego ruchu sieciowego z wzorcami aktywności normalnej
- Wzorce aktywności normalnej tworzone arbitralnie lub na podstawie danych historycznych
- Porównywane są wartości miar tworzonych na podstawie obserwowanego ruchu, na przykład:
  - ilość wysłanych do różnych portów segmentów SYN (w określonym przedziale czasu)
  - ilość segmentów z niewłaściwym numerem sekwencyjnym w sesji TCP

Wykrywanie anomalii – przykład

- Preprocesor sfPortscan systemu SNORT
- Wykrywa większość typów skanowania realizowanych przez aplikację NMAP
- Skanowanie typu SYN – do każdego portu skanowanego hosta wysyłany jest segment SYN
- Otwarte porty odpowiadają segmentem SYN ACK
- Zamknięte porty odpowiadają segmentem RST
- Sekwencja ACK, RST jest relatywnie rzadko spotykana w przypadku normalnego ruchu
- Wykrycie znacznej ilości takich sekwencji jest objawem skanowania portów

Reakcja

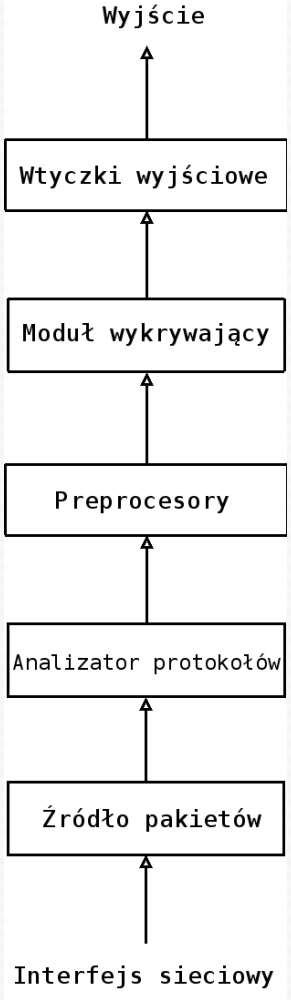
- Reakcja systemu na wykryty atak
- Reakcja aktywna:
  - Przerwanie sesji TCP przez wstrzyknięcie segmentu RST
  - Zablokowanie ruchu na firewallu
- Reakcja pasywna:
  - Zapis powiadomienia do dziennika systemowego
  - Wyświetlenie powiadomienia na konsoli zarządzania
  - Wysłanie wiadomości SMS lub e-mail

System wykrywania włamań Snort

- Open source
- Wykrywanie włamań przez dopasowywanie wzorców
- Wykrywanie anomalii realizowane przez preprocesory
- Brak wbudowanego interfejsu graficznego do zarządzania

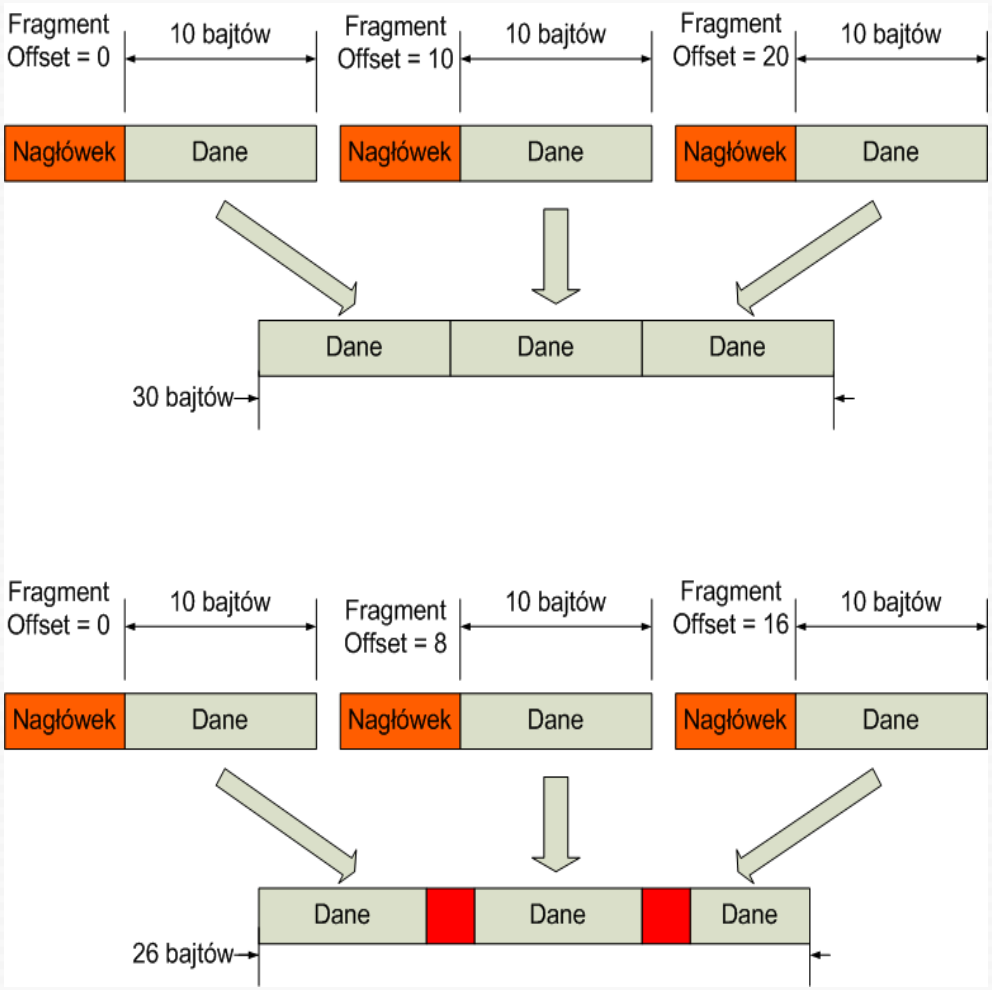
Architektura Snort

- Źródło pakietów libpcap lub iptables
- Preprocesory – rekonstrukcja pakietów, sesji, analiza statystyczna, wykrywanie specyficznych ataków
- Moduł wykrywający – reguły Snort
- Wtyczki wyjściowe – zapis do różnego rodzaju mediów, w różnych formatach

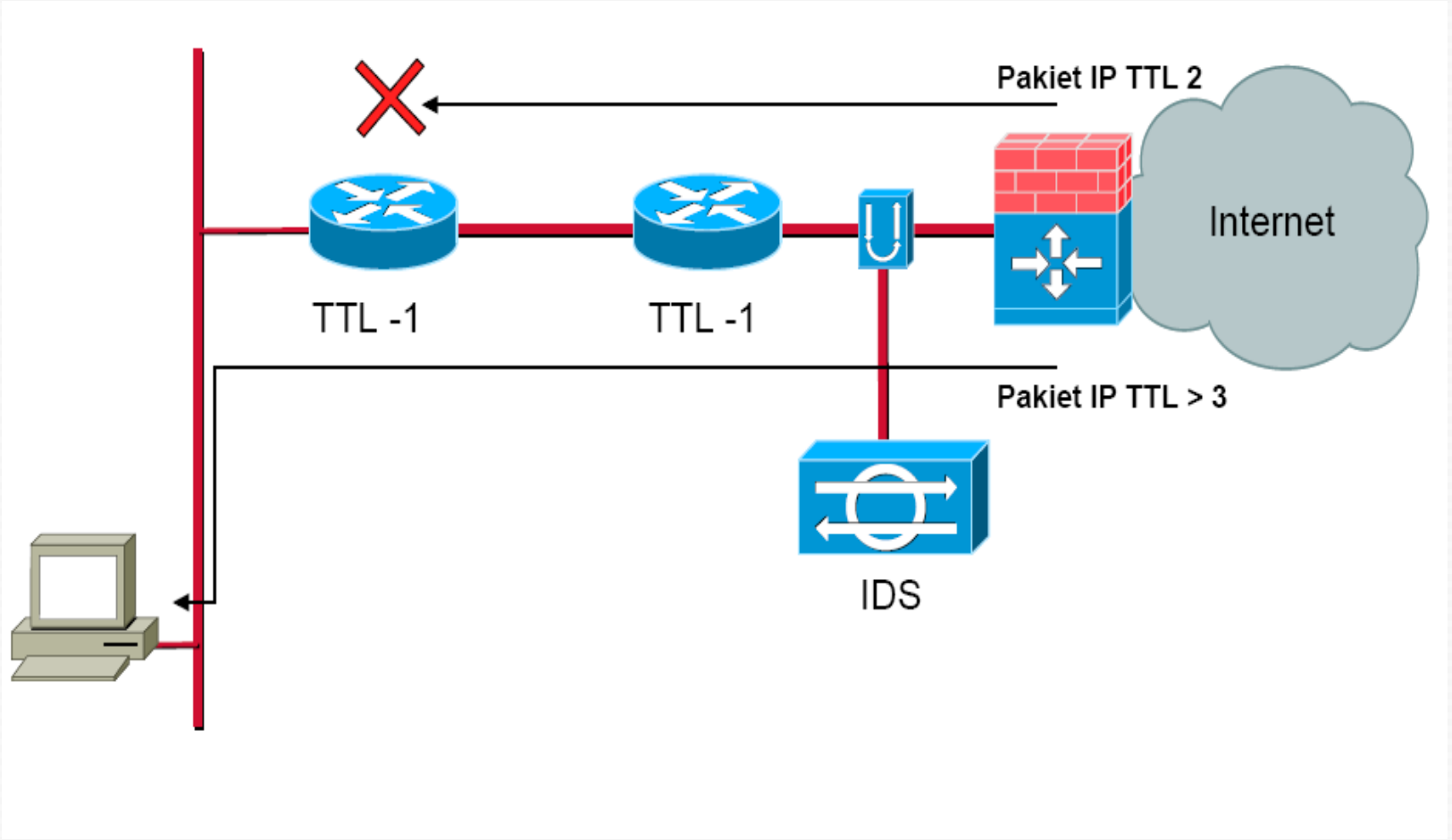


Preprocesory Snort - Frag3

- Rekonstrukcja pakietów do postaci otrzymywanej przez host docelowy
- Wykrywa ataki wykorzystujące odmienne polityki rekonstrukcji fragmentów oraz ataki oparte na mechaniźmie TTL
- Sposób rekonstrukcji oraz minimalna wartość pola TTL przypisywane do hostów



Preprocesory Snort - Frag3



Preprocesory Snort

- State4 – monitoruje stan połączeń TCP i zapobiega atakom typu *squealing* (Stick, Snot)
- sfPortscan – wykrywa większość typów skanowania portów
- HTTP Inspect
- FTP/Telnet
- SSH
- DNS
- DCE/RPC

Moduł wykrywający

- sygnatury specyfikowane za pomocą definicji o następującym formacie:

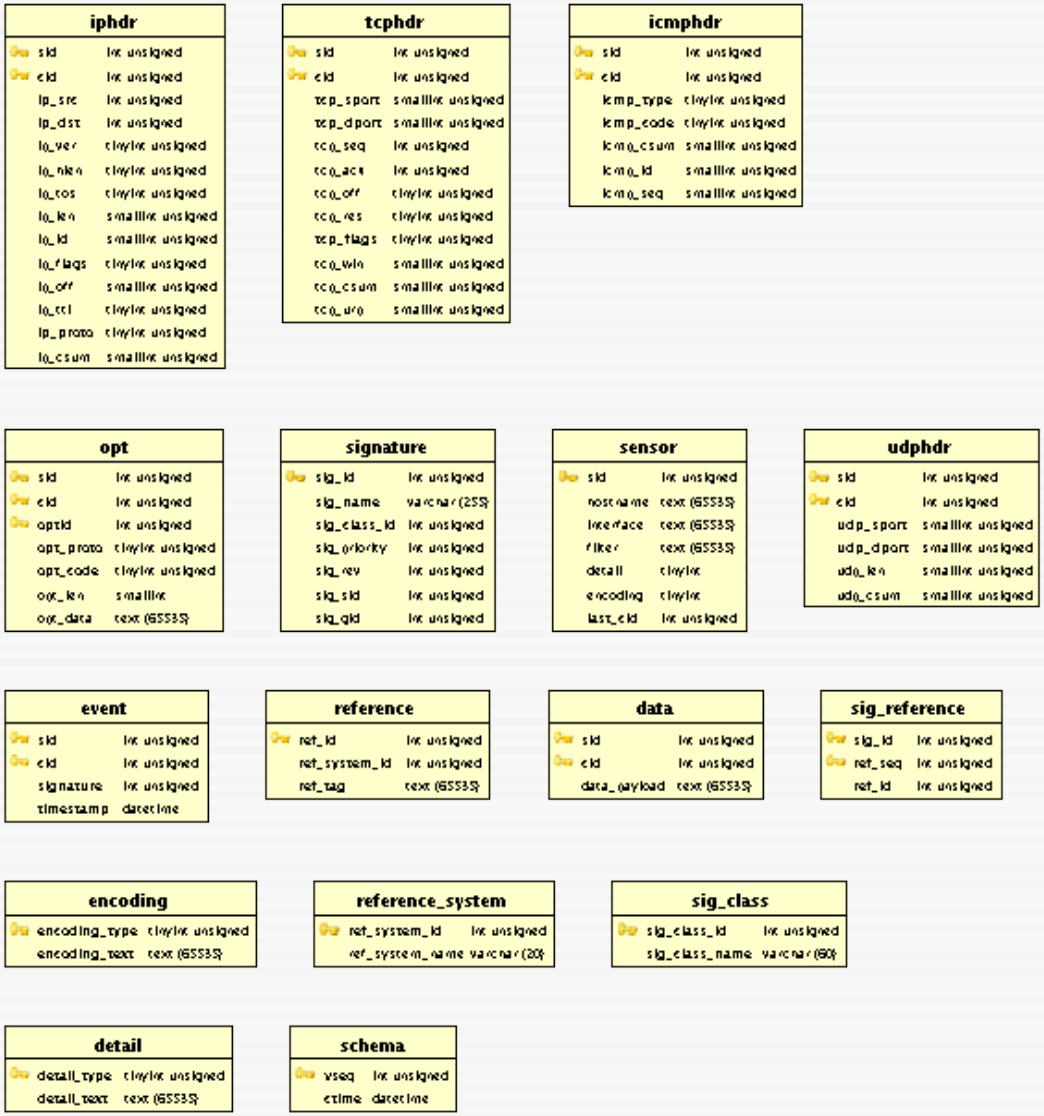
```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
(msg:"WEB-ATTACKS /bin/ps command attempt";
flow:to_server,established; uricontent:"/bin/ps"; nocase;
classtype:web-application-attack; sid:1328; rev:6;)
```

- podstawowe rodzaje akcji: alert, log, pass, activate, dynamic, drop, reject, sdrop
- możliwość definiowania własnych akcji:

```
ruletype redalert
{
    type alert
    output alert_syslog: LOG_AUTH LOG_ALERT
    output database: log, mysql, user=snort dbname=snort host=localhost
}
```

Wtyczki wyjściowe

- syslog
- plik
- UNIX domain socket
- tcpdump
- baza danych
- unified
- prelude



Zarządzanie systemem NIDS

- Zarządzanie działaniem sensorów
- Analiza, przeszukiwanie i wizualizacja wyników działania sensorów
- Współpraca z innymi elementami infrastruktury sieciowej

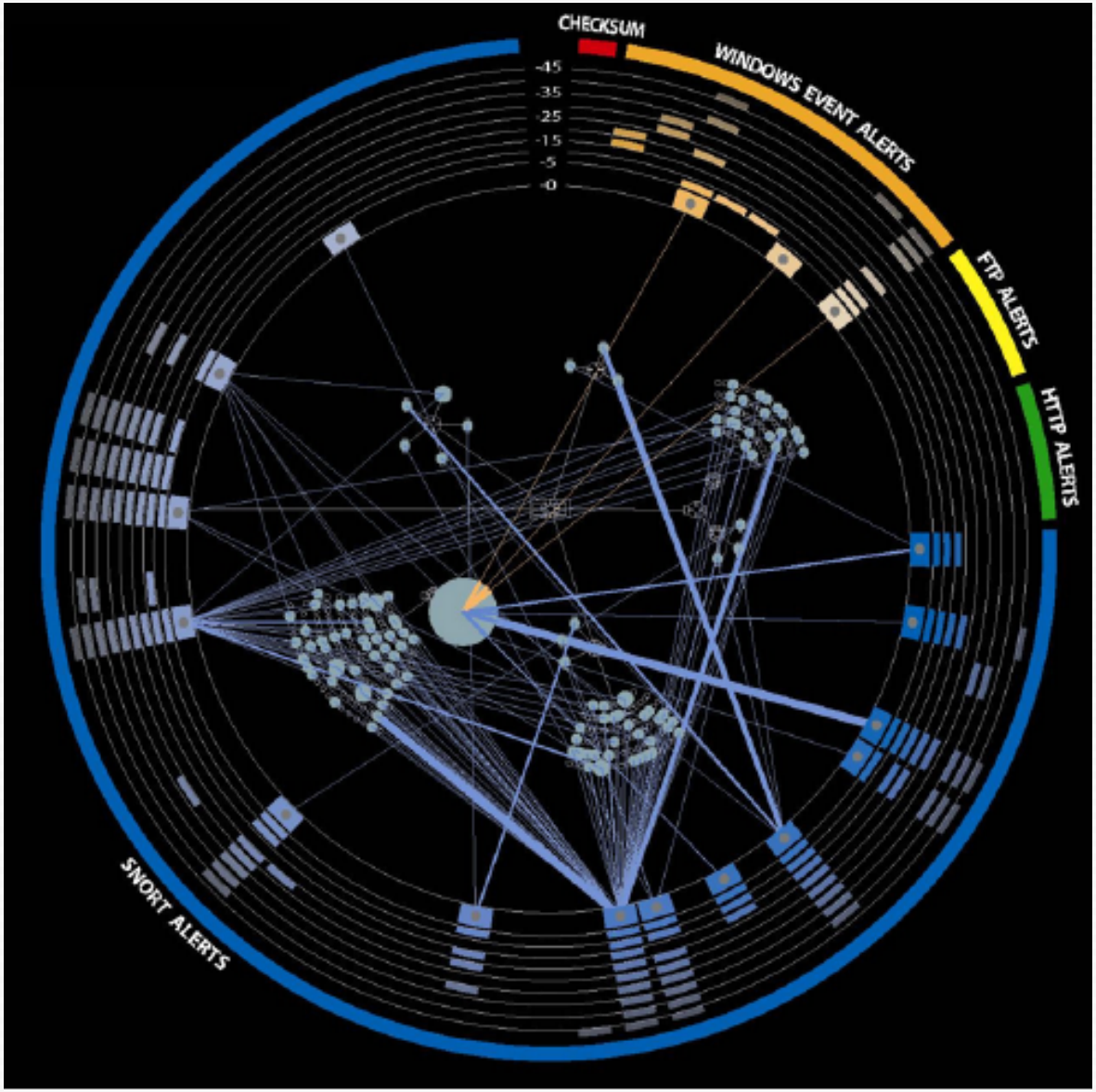
Zarządzanie działaniem sensorów

- Przypisywanie sygnatur do określonych sensorów
- Konfiguracja środowiska
- Konfiguracja sensora
- Monitorowanie działania sensora

Analiza, przeszukiwanie i wizualizacja powiadomień

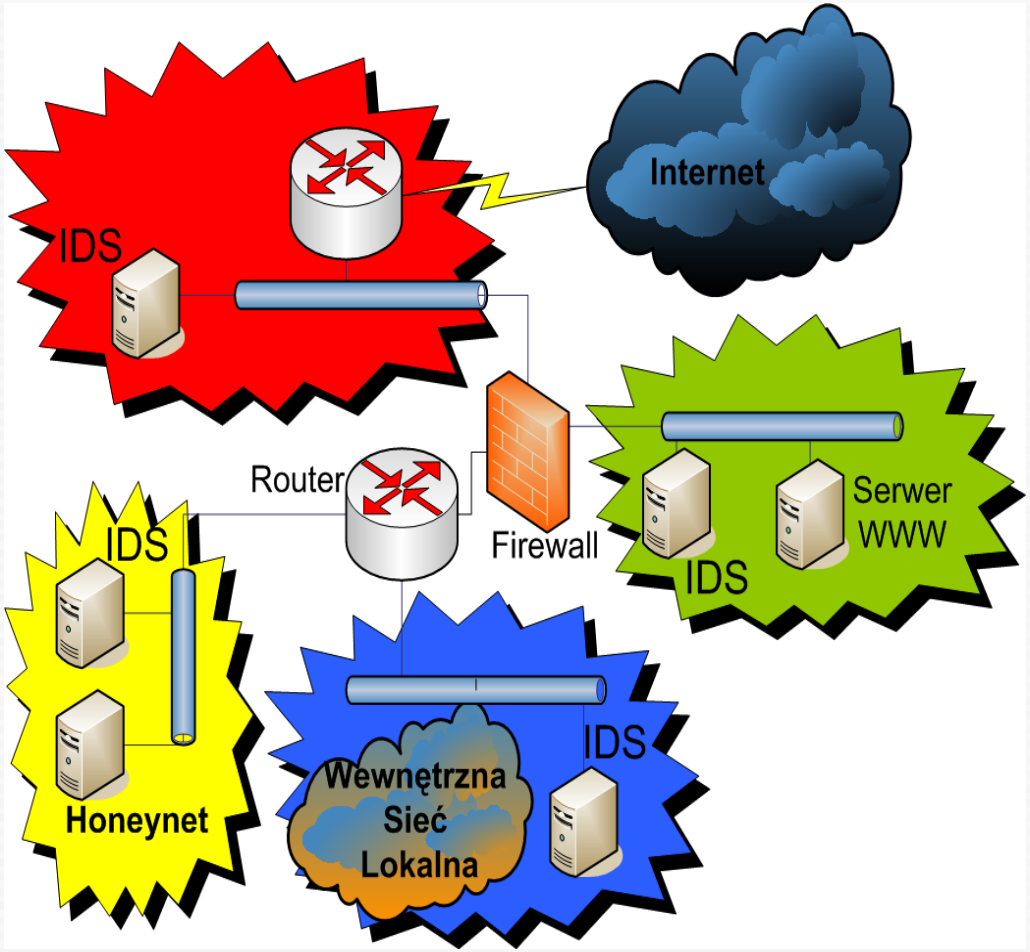
- Przeglądanie powiadomień w postaci listy
- Filtrowanie i sortowanie listy powiadomień
- Przeszukiwanie za pomocą słów kluczowych (*full text search*)
- Oznaczanie powiadomień
- Wizualizacja powiadomień

Analiza, przeszukiwanie i wizualizacja powiadomień



Analiza, przeszukiwanie i wizualizacja powiadomień

- różne wagi powiadomień dla sensorów umieszczonych w różnych strefach
- korelacja między powiadomieniami z różnych sensorów
- korelacja z innymi źródłami wiedzy (skanery portów, skanery podatności, systemy HIDS)



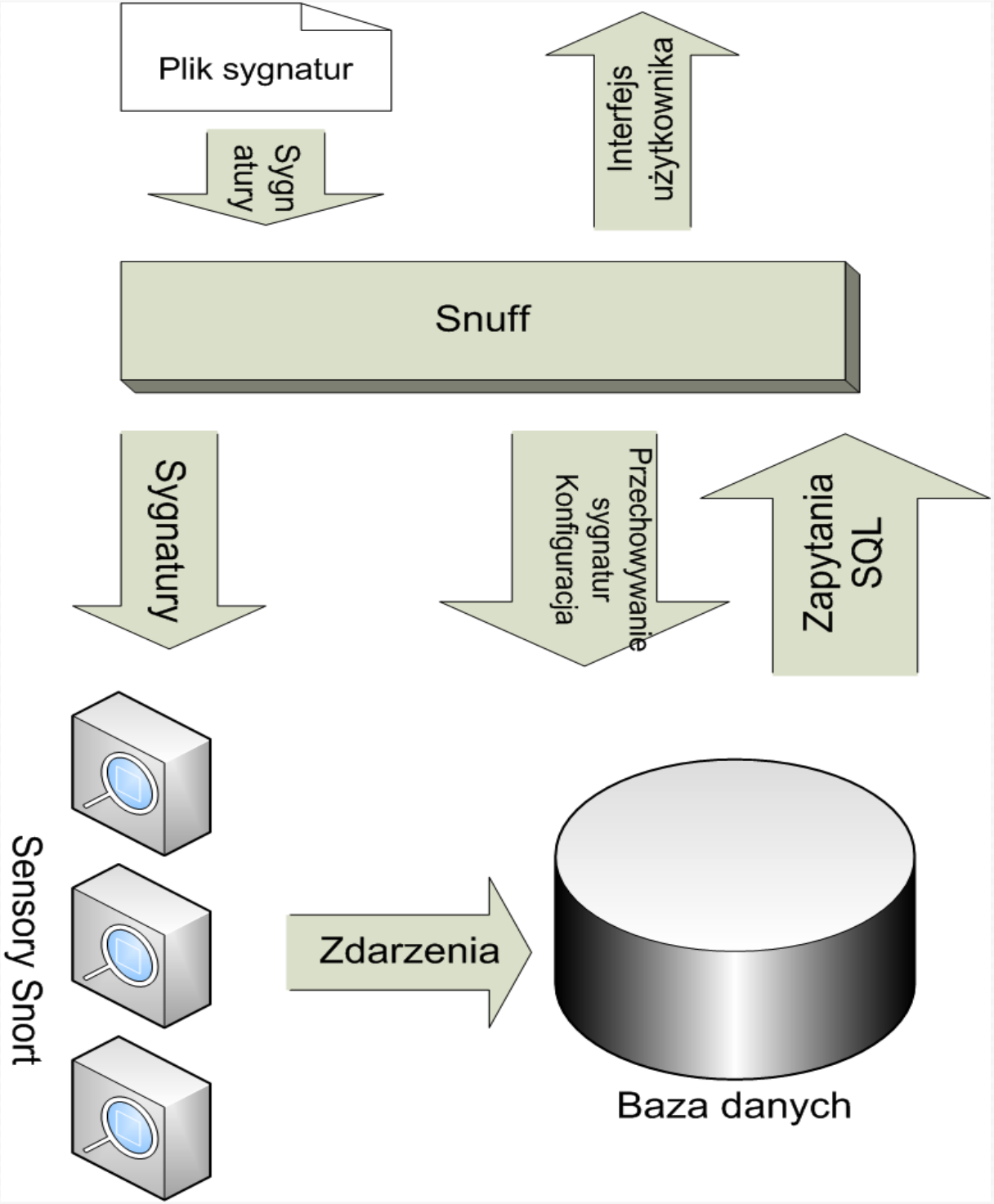
Współpraca z innymi elementami infrastruktury sieciowej

- umieszczanie reguł na firewallu stworzonych na podstawie alarmów/sygnatur
- odcinanie hostów na poziomie przełączników
- IPS – blokowanie ataków na poziomie sensora

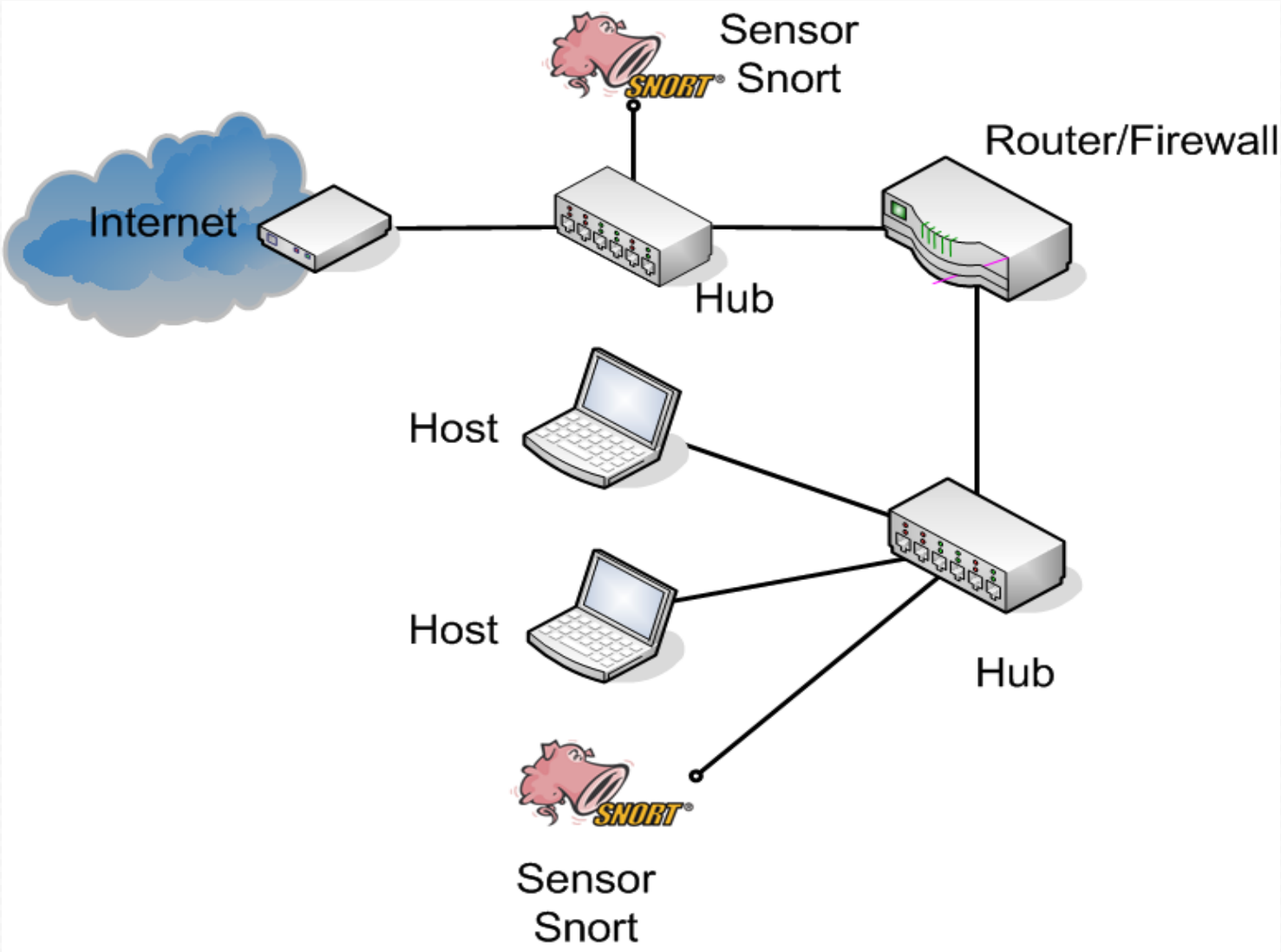
Cel pracy

- Stworzenie aplikacji umożliwiającej zarządzanie systememem wykrywania włamań Snort:
  - Graficzny interfejs użytkownika
  - Zarządzanie zbiorem sygnatur
  - Zarządzanie pracą sensorów
  - Przeglądanie, przeszukiwanie, wizualizacja i analiza powiadomień

Schemat systemu



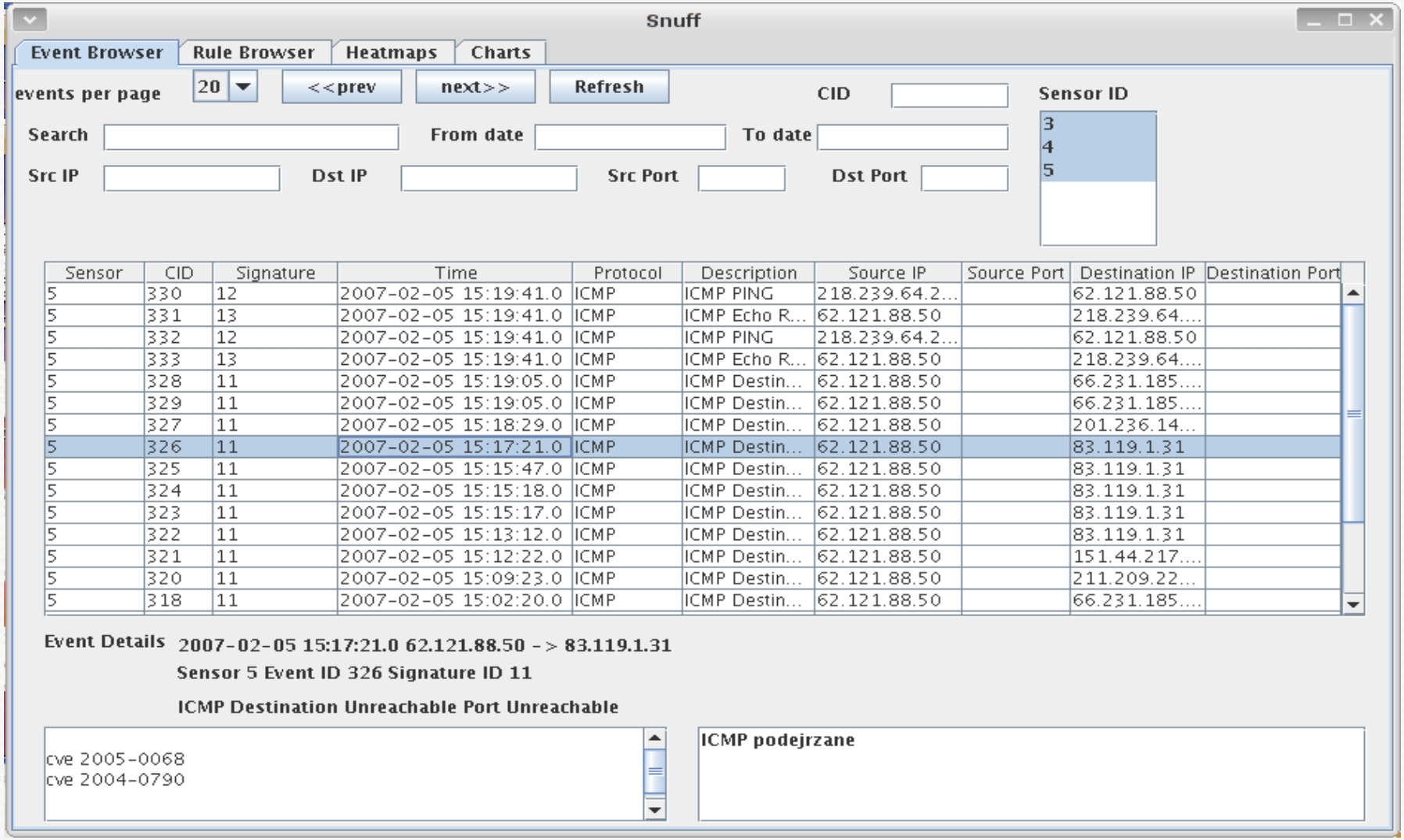
Środowisko Testowe



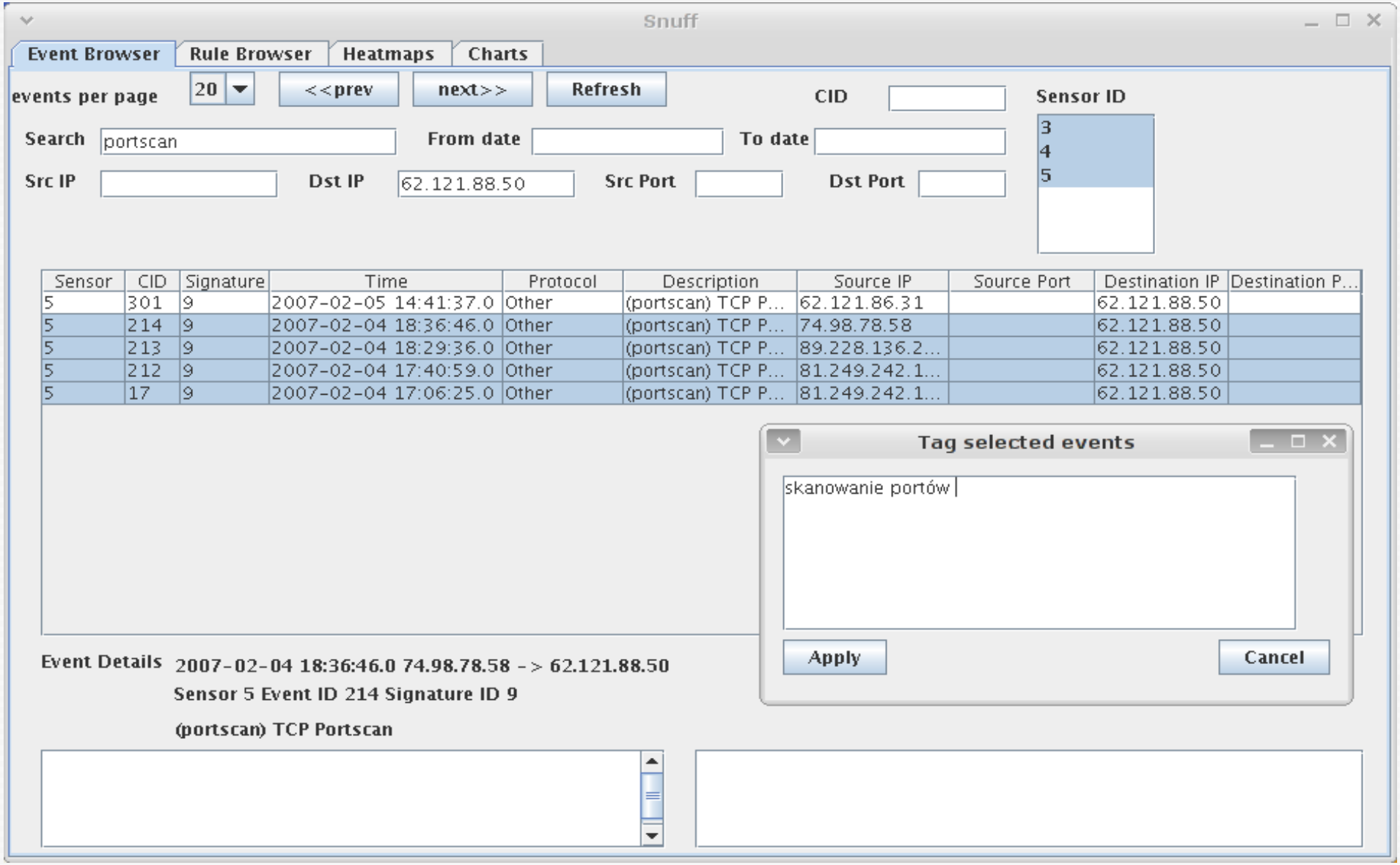
Przeglądanie i opisywanie alarmów

- Zapytania SQL
- Filtrowanie:
  - czas
  - źródłowe i docelowe adresy IP i porty TCP/UDP
  - sensory
- Przeszukiwanie pełnotekstowe po opisie sygnatury i opisach użytkownika
- Opisywanie alarmów – opisy przechowywane w dodatkowej tablicy

Przeglądanie alarmów



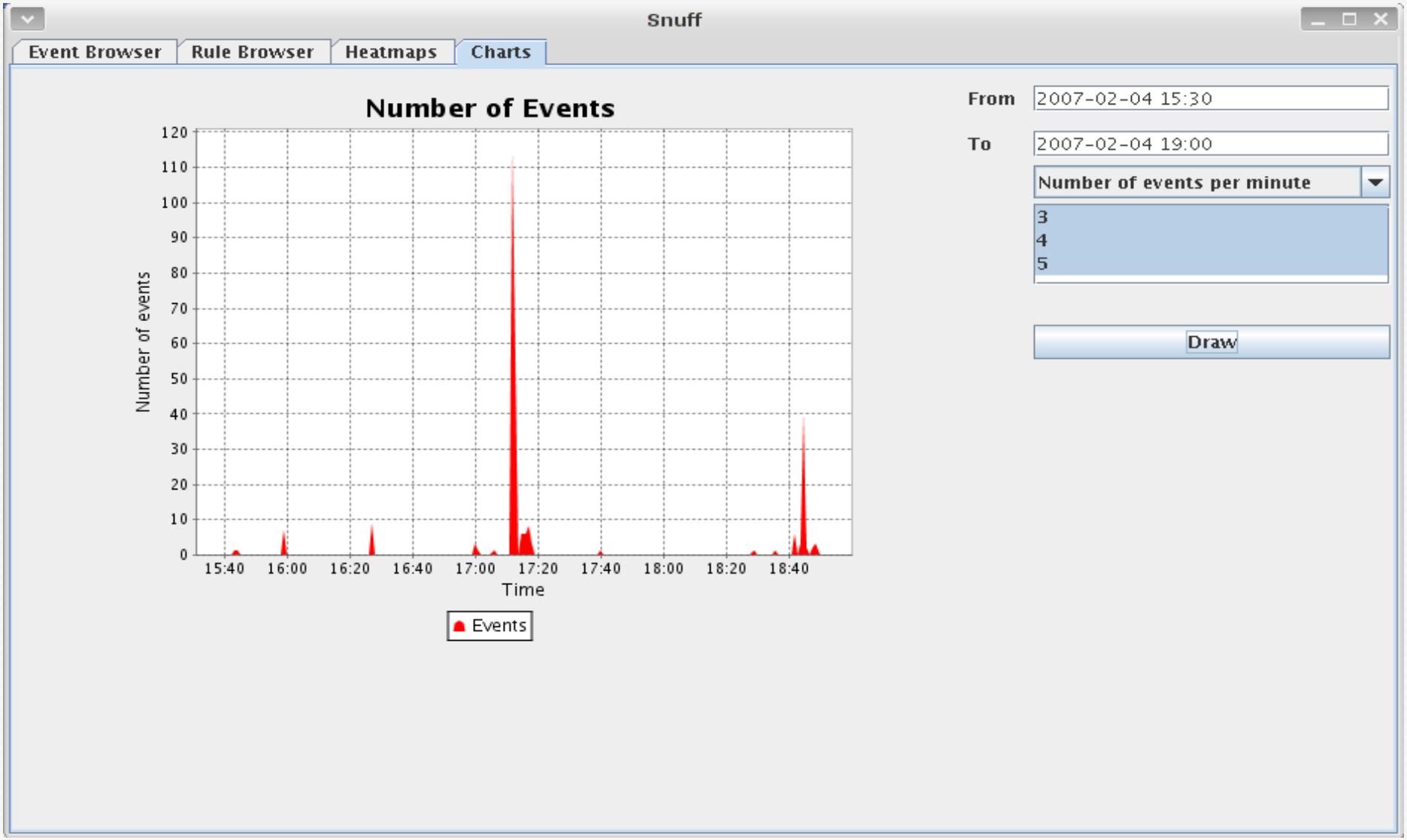
Opisywanie alarmów



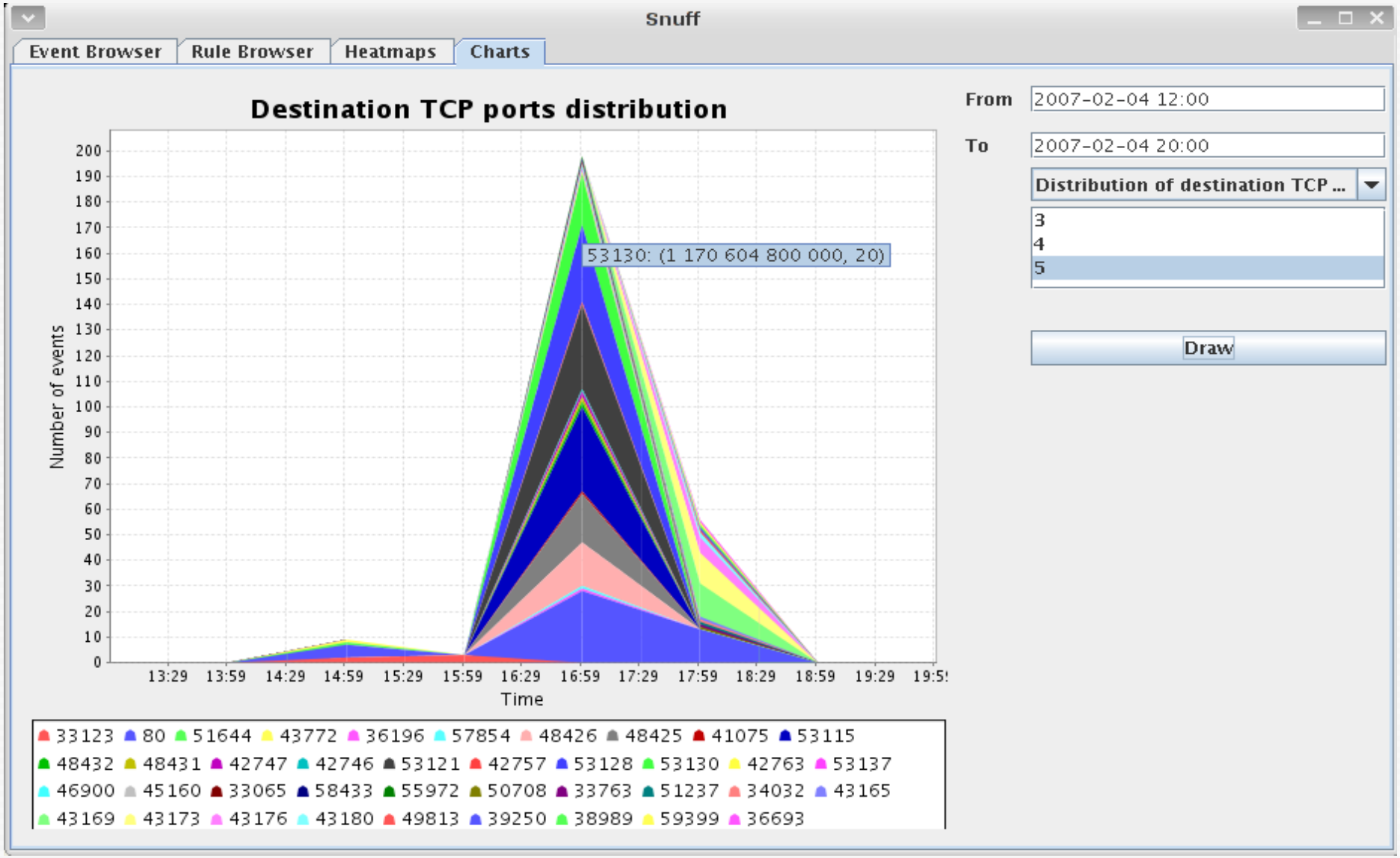
Wykresy

- Biblioteka JFreeChart
- Możliwość skalowania wykresu, zapisu do pliku
- Słupkowe wykresy liczby zdarzeń z rozdzielczością minutową, godzinową i dzienną
- Warstwowe wykresy akumulacyjne przedstawiające rozkład źródłowych i docelowych adresów IP i portów TCP/UDP

Wykresy


Snuff
Event Browser
Rule Browser
Heatmaps
Charts
Number of Events
Number of events
120
110
100
90
80
70
60
50
40
30
20
10
0
15:40
16:00
16:20
16:40
17:00
17:20
17:40
18:00
18:20
18:40
Time
Events
From
2007-02-04 15:30
To
2007-02-04 19:00
Number of events per minute
3
4
5
Draw

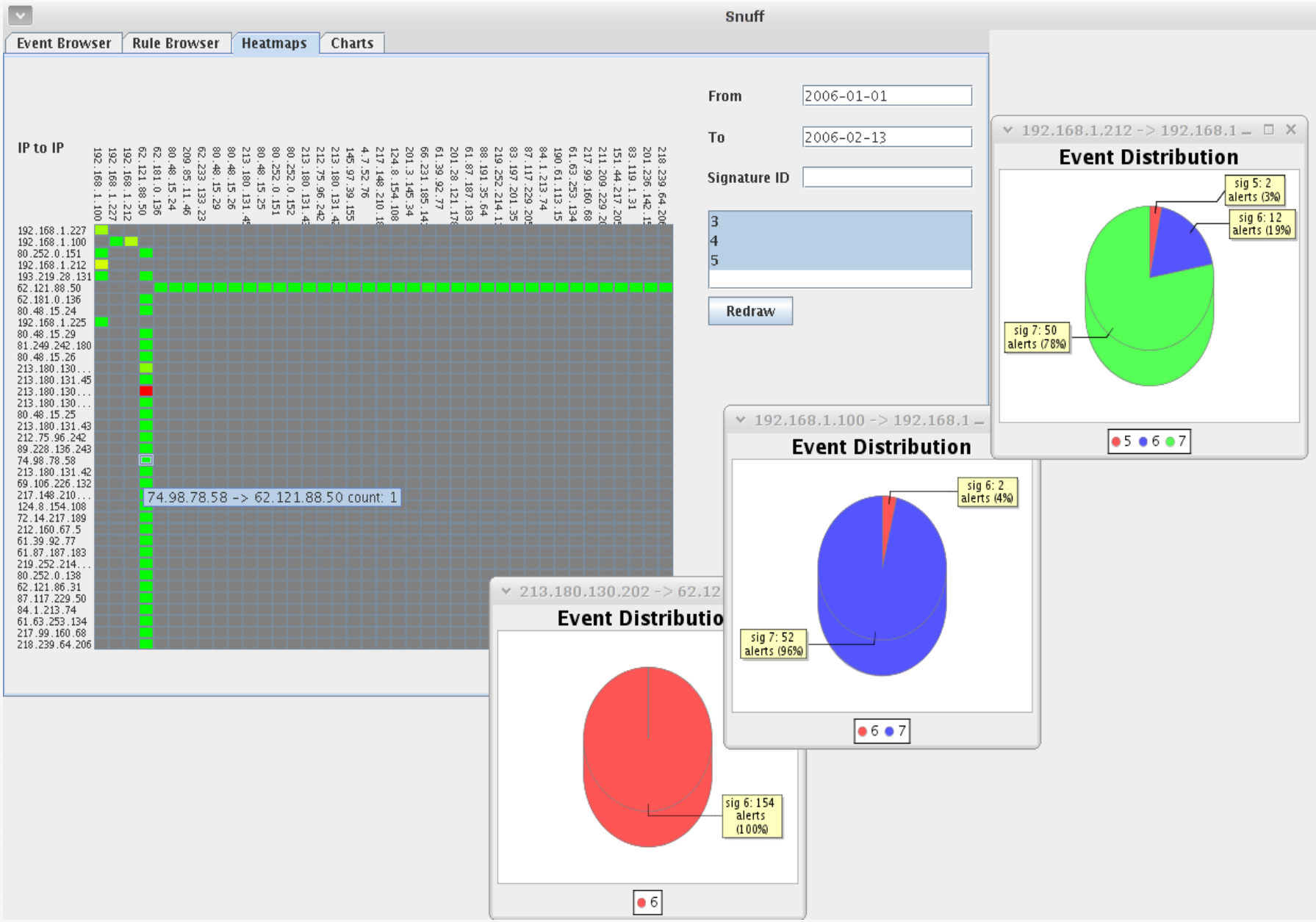
Wykresy


Snuff
Event Browser
Rule Browser
Heatmaps
Charts
Destination TCP ports distribution
53130: (1 170 604 800 000, 20)
Number of events
Time
From
2007-02-04 12:00
To
2007-02-04 20:00
Distribution of destination TCP ...
3
4
5
Draw
33123 80 51644 43772 36196 57854 48426 48425 41075 53115
48432 48431 42747 42746 53121 42757 53128 53130 42763 53137
46900 45160 33065 58433 55972 50708 33763 51237 34032 43165
43169 43173 43176 43180 49813 39250 38989 59399 36693

Mapa cieplna

- Rodzaj wykresu przedstawiający wartość funkcji dwóch zmiennych
- Liczba zdarzeń w funkcji źródłowego i docelowego adresu IP
- Rozkład rodzajów zdarzeń o zadanym źródłowym i docelowym adresie IP

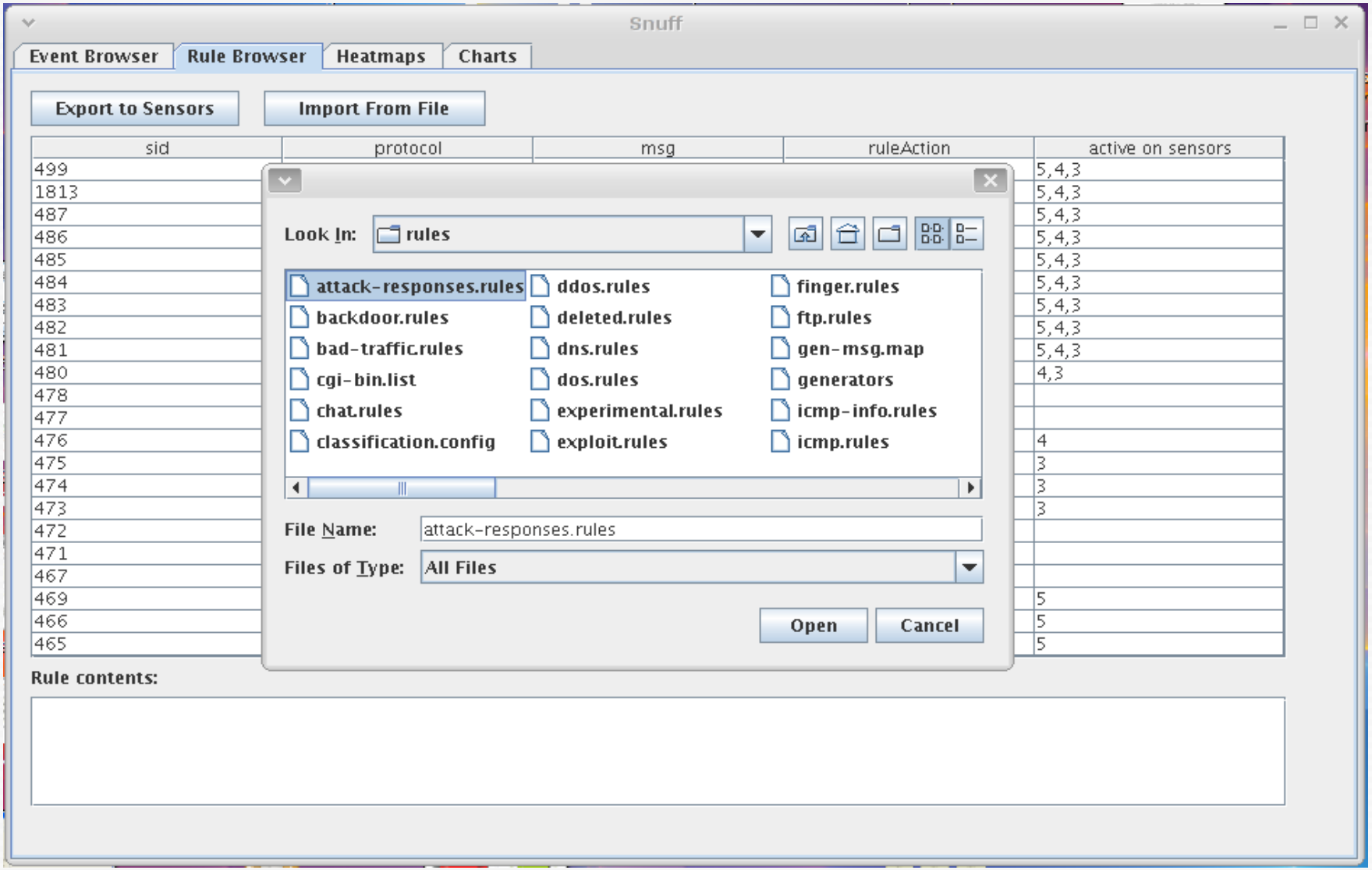
Mapa cieplna



Zarządzanie zbiorem sygnatur

- Sygnatury wczytywane z pliku do bazy danych
- Transport sygnatur na sensory za pomocą FTP
- Restartowanie sensorów za pomocą Telnetu

Zarządzanie zbiorem sygnatur



Perspektywy rozwoju

- Archiwizacja alarmów
- Ulepszenie interfejsu graficznego
- Zarządzanie konfiguracją sensorów
- SFTP i SSH zamiast FTP i Telnet
- Rozszerzone funkcje zarządzania sygnaturami (grupowanie w kategorie, filtrowanie, edytor sygnatur)
- Użycie modułu wyjściowego *unified*

Intrusion Detection Message Exchange Format

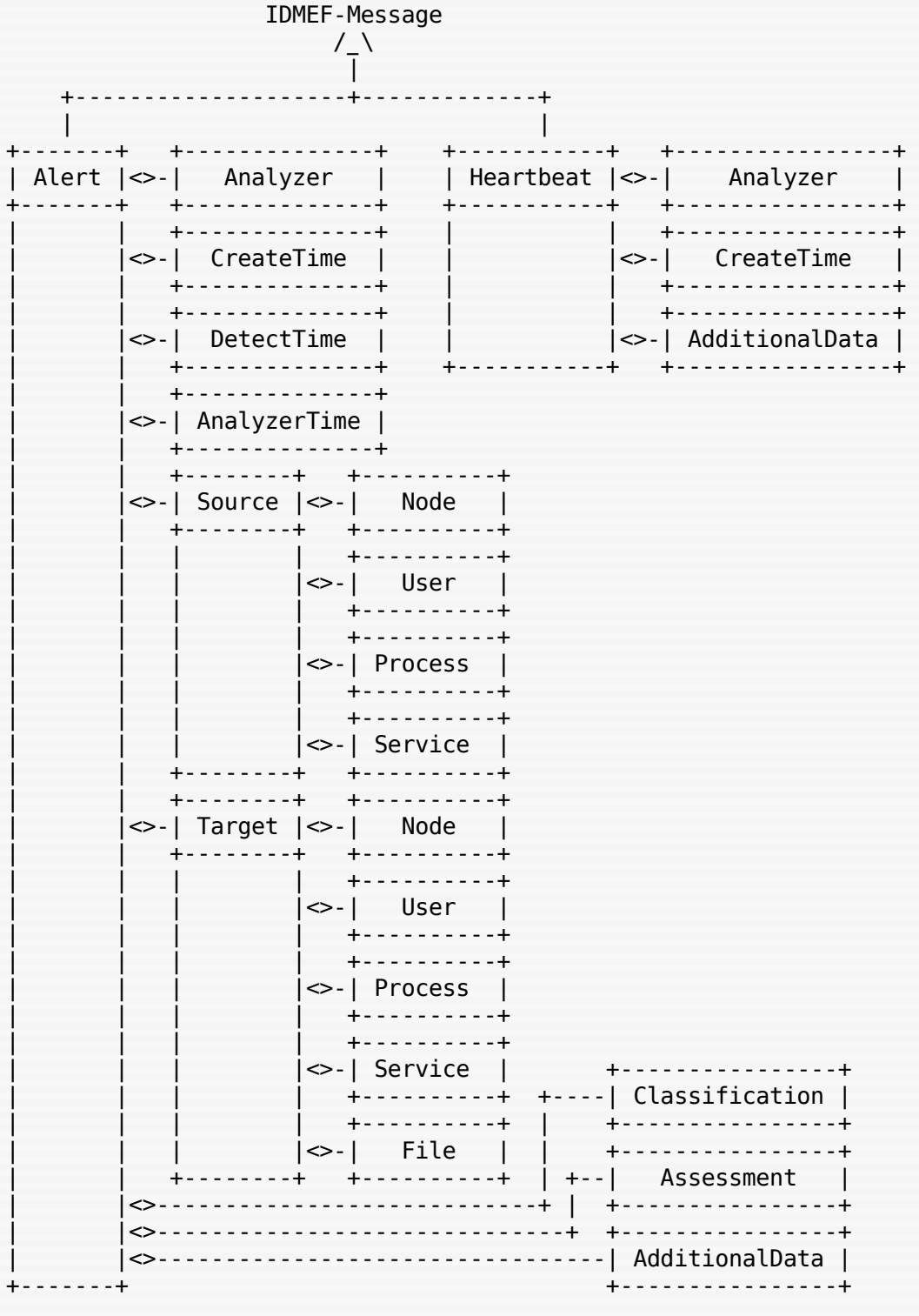
Intrusion Detection Message Exchange Format

- Experimental RFC 4765 (Listopad 2006)
- Standardyzacja formatu wiadomości generowanych przez systemy wykrywania włamań
- Cel: umożliwienie współpracy między komercyjnymi, otwartym i eksperymentalnymi systemami wykrywania włamań
- Wykorzystanie:
  - wymiana wiadomości między sensorami a centralną bazą danych
  - system korelujący powiadomienia z różnego typu sensorów
  - graficzne konsole zarządzania

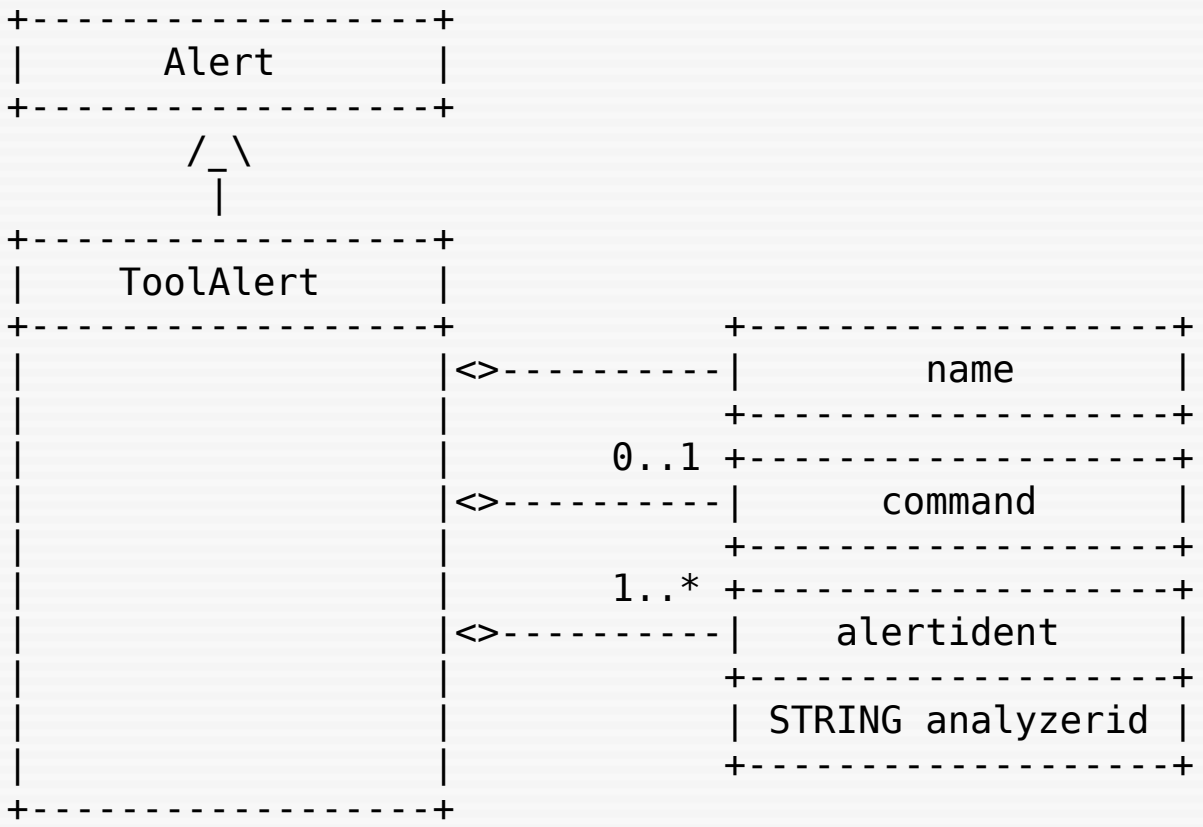
Intrusion Detection Message Exchange Format

- Heterogeniczne sensory – różna ilość, szczegółowość, rodzaj informacji zawartych w powiadomieniach
- Rozwiązanie: model powiadomień zorientowany obiektowo, umożliwiający rozszerzanie i dziedziczenie klas
- Definicja formatu w XML

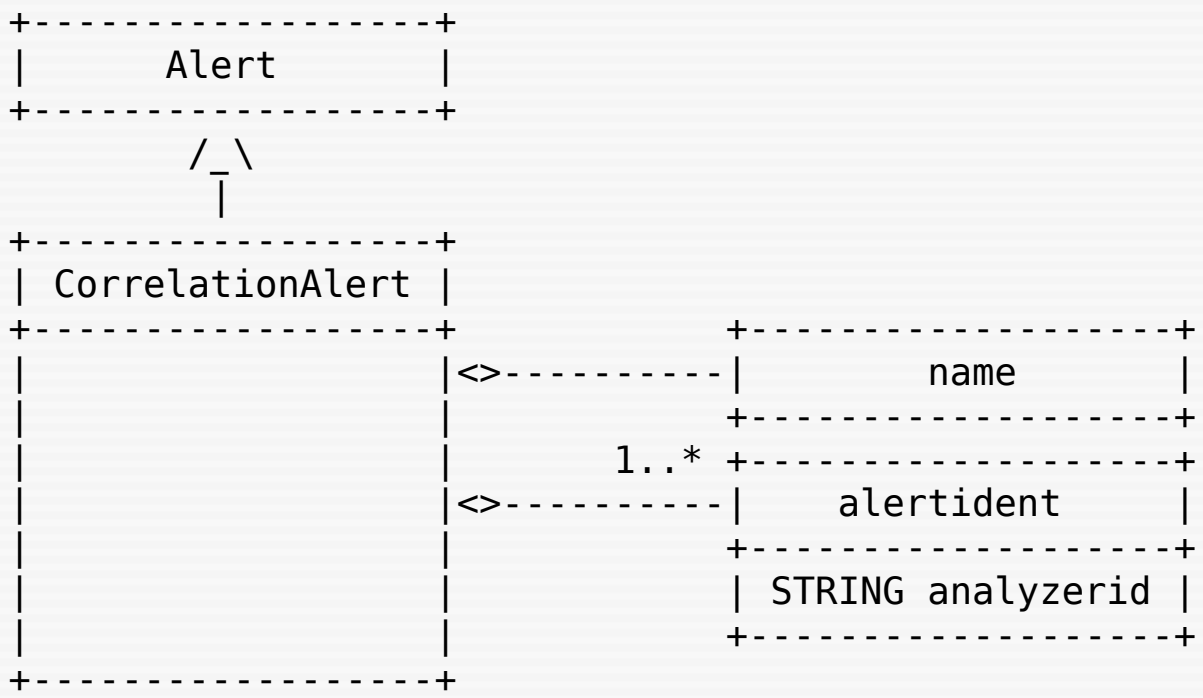
IDEMF – model danych



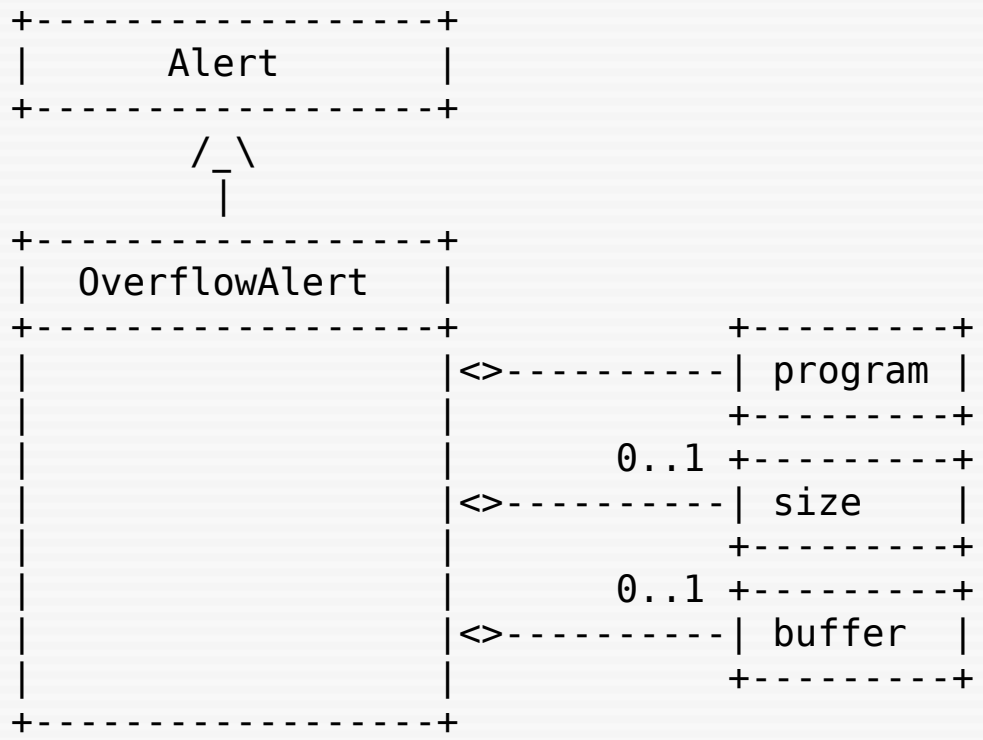
IDEMF – Tool Alert



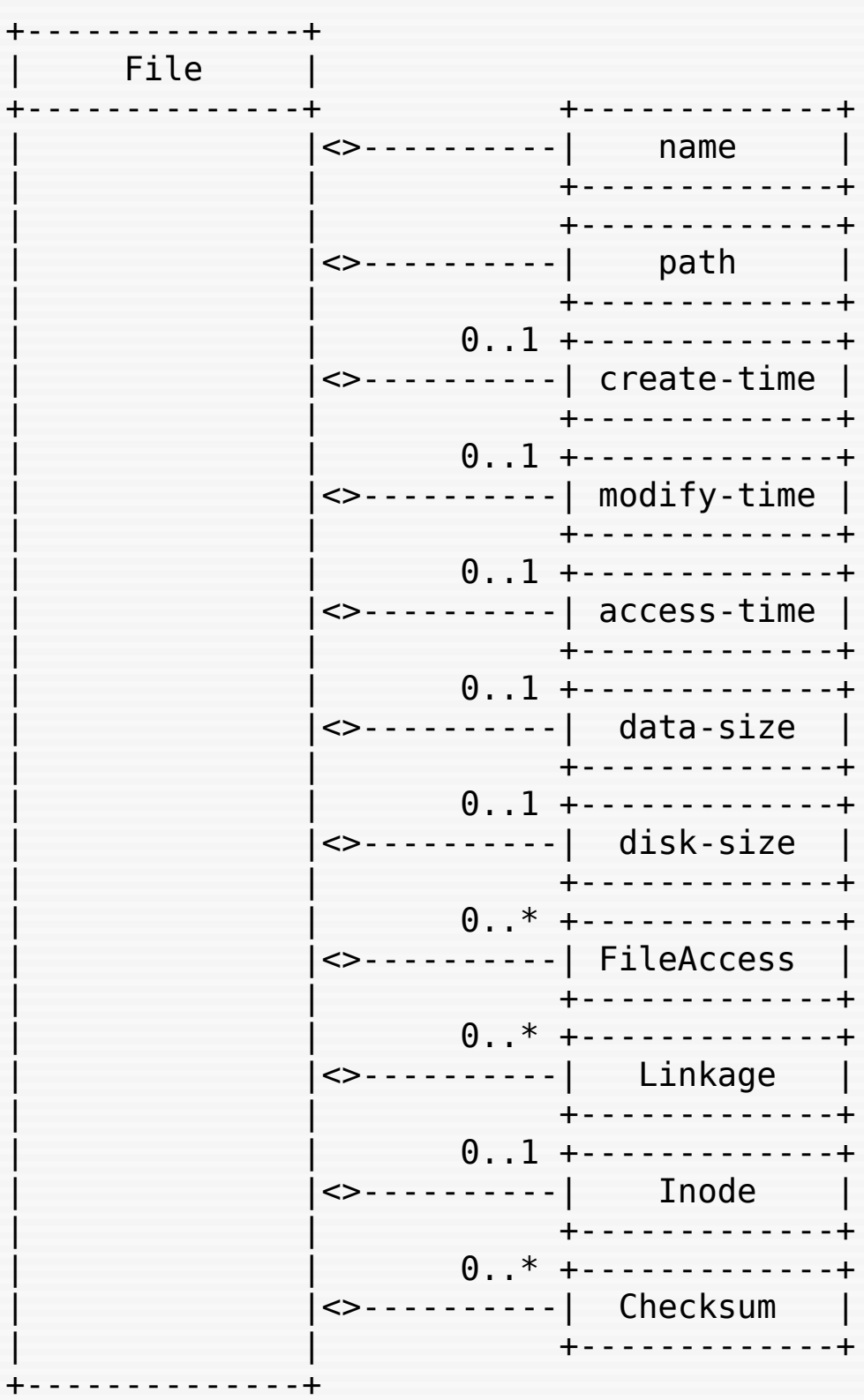
IDEMF – Correlation Alert



IDEMF – Overflow Alert



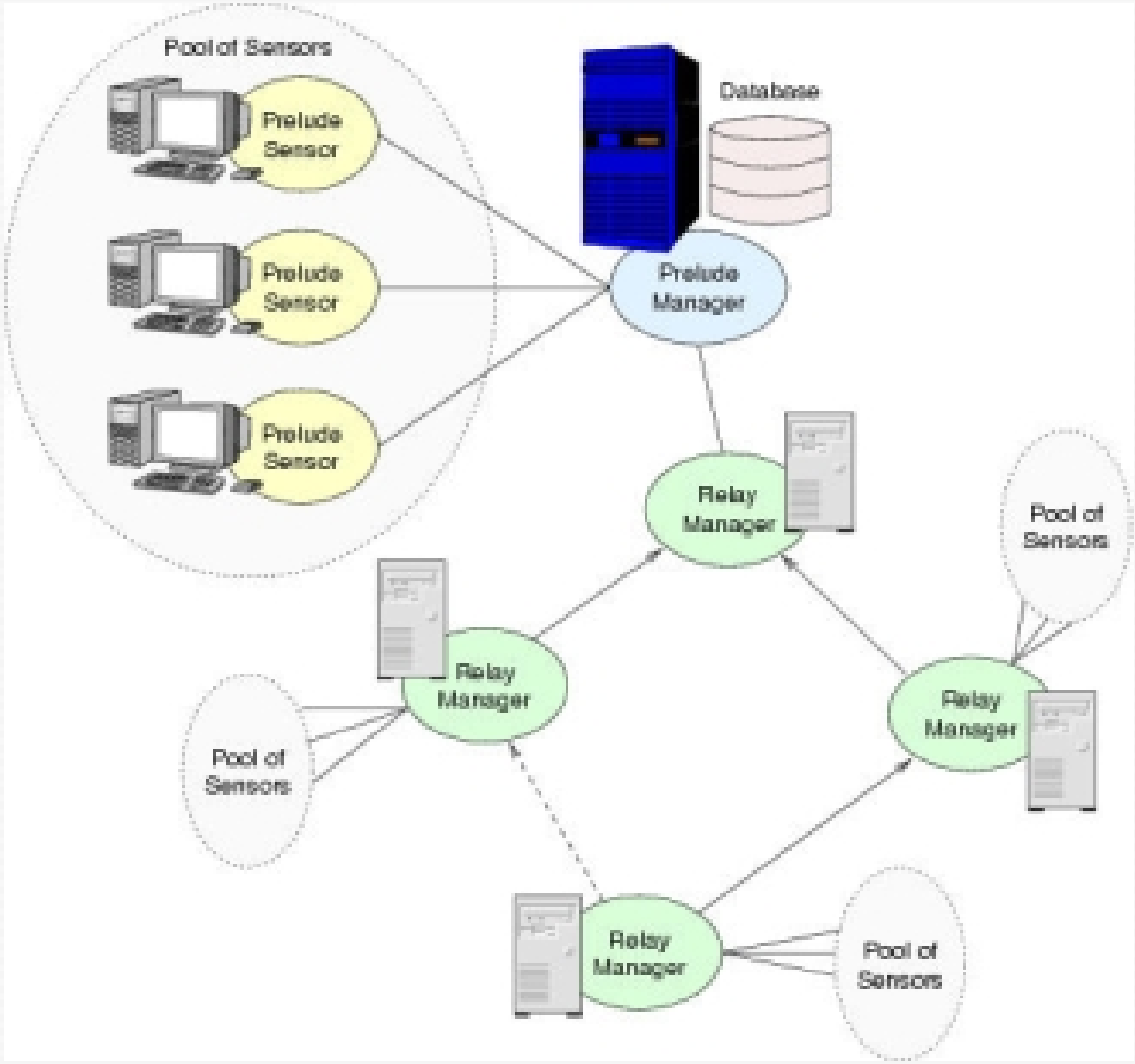
IDEMF – Klasa File



Prelude IDS

- Hybrydowy system wykrywania włamań wykorzystujący standard IDEMF
- GPL v2
- Wiele rodzajów sensorów
- Możliwość wykorzystania sensorów spoza projektu Prelude

Prelude - architektura



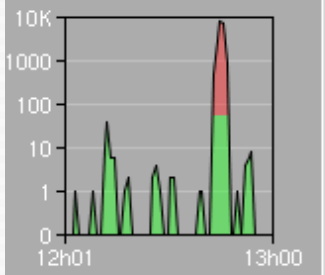
Sensory kompatybilne z Prelude

- Prelude:
  - Prelude LML – analiza logów
  - Prelude NIDS
  - Prelude-pflogger – powiadomienia z BSD Packet Filter
- Pozostałe:
  - Snort
  - systrace – monitoruje wywołania syscalli
  - honeyd - honeypot
  - Nessus – skaner podatności
  - Samhain – sumy kontrolne
  - libsafe – zapobiega przepełnieniu bufora
  - sancp – statystyki ruchu sieciowego

PreludeIDS Technologies. **Prelude-IDS console**

Alerts | Heartbeats | Filters — *yoann*, on Monday March 07 2005 — logout

- Events
- Agents
- Users
- Settings
- Stats
- About



Sensors availability:

3 | 1

Filter:
Step: 1 Hours
Tz: Frontend localt
Limit: 50 apply

2005-03-07 12:01:51
2005-03-07 13:01:51
+01:00

prev | current | next

1 ... 43 (total:43)

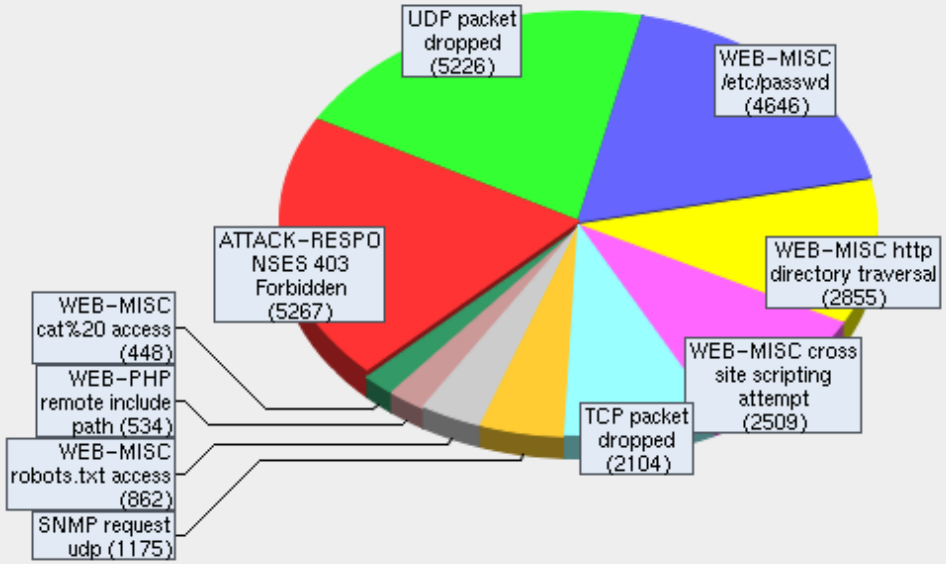
Classification	Source	Target	Sensor	Time	
WEB-MISC robots.txt access	84.104.217.36:45295	194.246.101.65:80	snort (on awale.prelude-ids.org)	13:01:07	☐
2 x TCP packet dropped (failed)	216.184.192.227:2927	194.246.101.67:139 interface: eth1	prelude-lml/netfilter (on awale.prelude-ids.org)	12:54:56 - 12:54:53	☐
6 x TCP packet dropped (failed)	200.14.104.27:57332	194.246.101.65:113 interface: eth1	prelude-lml/netfilter (on awale.prelude-ids.org)	12:54:42 - 12:53:09	☐
2 x TCP packet dropped (failed)	194.246.104.67:1924	194.246.101.67:445 interface: eth1	prelude-lml/netfilter (on awale.prelude-ids.org)	12:54:35 - 12:54:32	☐
TCP packet dropped (failed)	212.22.171.145:63721	194.246.101.65:139 interface: eth1	prelude-lml/netfilter (on awale.prelude-ids.org)	12:54:08	☐
TCP packet dropped (failed)	212.22.171.145:63722	194.246.101.66:139 interface: eth1	prelude-lml/netfilter (on awale.prelude-ids.org)	12:54:08	☐
TCP packet dropped (failed)	212.22.171.145:63723	194.246.101.67:139 interface: eth1	prelude-lml/netfilter (on awale.prelude-ids.org)	12:54:08	☐
Mail server suspicious access (failed)	62.103.252.123	194.246.101.65 (awale.prelude-ids.org)	prelude-lml/Postfix (on awale.prelude-ids.org)	12:53:01	☐
5 x TCP packet dropped (failed)	172.16.1.25:4170	194.246.101.65:445 interface: eth1	prelude-lml/netfilter (on awale.prelude-ids.org)	12:52:50 - 12:31:07	☐
2 x TCP packet dropped (failed)	172.16.1.25:2690	194.246.101.66:445 interface: eth1	prelude-lml/netfilter (on awale.prelude-ids.org)	12:52:18 - 12:52:15	☐
WEB-MISC robots.txt access	68.142.250.85:43652	194.246.101.65:80	snort (on awale.prelude-ids.org)	12:50:52	☐
(14910/15088 alerts not shown... expand) 6 x **(spo_bo) Back Orifice Traffic detected** 2 x **TFTP GET passwd** 8 x **WEB-CGI /cgi-bin/ access** 40 x **WEB-CGI a1stats a1disp3.cgi directory traversal attempt** 1 x **WEB-CGI agora.cgi attempt** 20 x **WEB-CGI AltaVista Intranet Search directory traversal attempt** 20 x **WEB-CGI Amaya templates sendtemp.pl directory traversal attempt** 41 x **WEB-CGI anaconda directory transversal attempt** 20 x **WEB-CGI Armada Style Master Index directory traversal** 20 x **WEB-CGI auktion.cgi directory traversal attempt**	82.226.58.44	194.246.101.65:22 (awale.prelude-ids.org)	prelude-lml/sshd (on awale.prelude-ids.org)	12:47:22 - 12:43:21	☐
2630 x ATTACK-RESPONSES 403 Forbidden	194.246.101.65:80	82.226.58.44:38669	snort (on awale.prelude-ids.org)	12:47:21 - 12:43:55	☐

Done

Alerts categorization

Period: current month (from 2005/02/07 01:19 to 2005/03/07 01:19)

Top 10 Alert Classifications



Classification	Alerts Count	Percent
ATTACK-RESPONSES 403 Forbidden	5267	20.6 %
UDP packet dropped	5226	20.4 %
WEB-MISC /etc/passwd	4646	18.1 %
WEB-MISC http directory traversal	2855	11.1 %
WEB-MISC cross site scripting attempt	2509	9.8 %
TCP packet dropped	2104	8.2 %
SNMP request udp	1175	4.6 %
WEB-MISC robots.txt access	862	3.4 %
WEB-PHP remote include path	534	2.1 %
WEB-MISC cat%20 access	448	1.7 %
Total	**25626**	**100.0 %**

Alert Severities

Severity	Alerts Count	Percent
medium	35940	83.8 %
high	6430	15.0 %
low	525	1.2 %
Total	**42895**	**100.0 %**

Filter:
Time: Month
From: 2005 / 02 / 07 01 : 19
To: 2005 / 03 / 07 01 : 19
apply

Done