

**Zarządzanie bezpieczeństwem systemów  
informatycznych  
- Juniper Security Threat Response Manager (STRM)**

**DEDYKOWANE WARSZTATY ZABEZPIECZEŃ**

Opracował: dr inż. Mariusz Stawowski  
CISSP, JNCIS

## **PROGRAM WARSZTÓW**

<b>WPROWADZENIE</b>	<b>3</b>
<b>1. ZASADY DZIAŁANIA STRM</b>	<b>4</b>
<b>2. ZARZĄDZANIE LOGÓW I OBSŁUGA INCYDENTÓW (SIEM)</b>	<b>6</b>
<b>3. WYKRYWANIE ANOMALII SIECI (NBAD)</b>	<b>7</b>
<b>4. MODELE I SCENARIUSZE WDROŻENIA STRM</b>	<b>8</b>
<b>5. PODSTAWOWA KONFIGURACJA I ADMINISTRACJA STRM</b>	<b>10</b>
<b>6. KONSOLA ZARZĄDZANIA DASHBOARD</b>	<b>16</b>
<b>7. PRZEGLĄDANIE ZDARZEŃ EVENT VIEWER</b>	<b>18</b>
<b>8. ZARZĄDZANIE INCYDENTÓW OFFENSE MANAGER</b>	<b>20</b>
<b>9. ANALIZA BEZPIECZEŃSTWA CHRONIONYCH ZASOBÓW (ASSETS)</b>	<b>25</b>
<b>10. ANALIZA STANU SIECI (FLOW VIEWER, NETWORK SURVEILLANCE)</b>	<b>26</b>
<b>11. INTEGRACJA STRM Z JUNIPER NSM I PROFILER</b>	<b>27</b>
<b>12. TWORZENIE STATYSTYK I RAPORTÓW</b>	<b>29</b>

## Wprowadzenie

Działalność biznesowa firm jest coraz mocniej uzależniona od systemów informatycznych. Efektywne zarządzanie ich bezpieczeństwem w skali całego przedsiębiorstwa staje się dużym wyzwaniem. Podstawowe wymagania stawiane systemom zarządzania bezpieczeństwem są następujące:

- w jednym miejscu obsługa incydentów bezpieczeństwa dla całego obszaru systemu informatycznego,
- zarządzanie i analiza wielu milionów rejestrowanych zdarzeń bez ponoszenia dużych nakładach pracy,
- precyzyjne monitorowanie stanu i efektywności pracy środowiska sieciowego (m.in. przeciążeń, awarii, ataków D/DoS i 0-day),
- spełnienie wymagań prawnych, standardów bezpieczeństwa i innych regulacji (PCI, SOX, ISO-27001, Basel II, itd.).

Rozwiązaniem spełniającym powyższe wymagania są systemy klasy **Security Information and Events Management (SIEM)** oraz **Network Behavior Anomaly Detection (NBAD)**. Systemy SIEM pobierają logi z wielu różnych elementów systemu informatycznego, poddają je korelacji i na tej podstawie przedstawiają administratorom wiarygodne informacje na temat stanu bezpieczeństwa i wykrytych incydentów. Logi z systemu informatycznego nie pokazują jednak pełnego obrazu bezpieczeństwa.

Podstawą prawidłowego funkcjonowania systemów informatycznych jest sieć. Od systemu zarządzania bezpieczeństwem wymagane jest precyzyjne monitorowanie stanu i efektywności pracy środowiska sieciowego. Takie zadania spełnia NBAD, który na podstawie statystyk i opisu ruchu (np. NetFlow) pobieranych bezpośrednio z urządzeń sieciowych (ruterów, przełączników) dokonuje analizy stanu i efektywności pracy sieci, w tym wykrywania sytuacji nieprawidłowych (anomali).

Utrzymywanie dwóch systemów zarządzania SIEM i NBAD zwiększa nakłady administracyjne i koszty utrzymania zabezpieczeń. Uzasadnione jest stosowanie rozwiązań zintegrowanych.

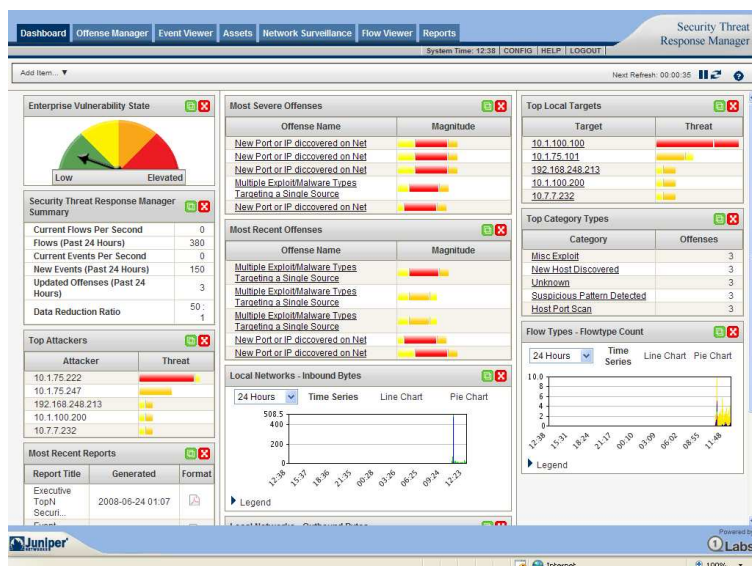
## 1. Zasady działania STRM

**Juniper Security Threat Response Manager (STRM)** to scentralizowany system zarządzania bezpieczeństwem realizujący funkcje SIEM i NBAD oraz utrzymujący centralne repozytorium logów. Juniper STRM obsługuje incydenty bezpieczeństwa na podstawie następujących źródeł informacji:

- **zdarzenia i logi z systemów zabezpieczeń** (firewall, VPN, IPS, AV, itd.), systemów operacyjnych (Unix, Windows, itd.) oraz aplikacji i baz danych,
- **statystyki i opis ruchu sieciowego** odbierane z urządzeń za pomocą NetFlow, J-Flow, S-Flow i Packeteer oraz odczytywane bezpośrednio z sieci (span port),
- **informacje na temat stanu systemów i ich słabości bezpieczeństwa** odczytywane za pomocą Juniper IDP Profiler oraz skanerów Nessus, NMAP, nCircle, Qualys, Foundstone, itd.

Zdarzenia i logi pobierane są przez STRM za pomocą różnych metod, m.in. **Syslog** – standardowy format logów (TCP, UDP), **SNMP** - wiadomości o zdarzeniach (SNMP Trap, v3), **Adaptive Log Exporter (ALE) Agent** - zdarzenia z systemów MS Windows, **JuniperNSM** – integracja z systemem zarządzania Juniper NSM, **JDBC:SiteProtector** – integracja z **IBM SiteProtector**, **Log Export API (LEA)** – integracja z systemem zarządzania **Check Point**, **Security Device Event Exchange (SDEE)** - protokół używany w urządzeniach **Cisco**, oparty na SOAP, a także **Java Database Connectivity API (JDBC)** - zdalny dostęp do baz danych.

Administratorzy bezpieczeństwa korzystają z STRM za pomocą dedykowanych, graficznych narzędzi uruchamianych z wykorzystaniem standardowej przeglądarki Web. Nie ma potrzeby instalowania do tego celu dodatkowych aplikacji. STRM wspiera przeglądarki Microsoft Internet Explorer 7.0 i Firefox 2.0 (oraz ich nowsze wersje).



*Konsola zarządzania Juniper STRM*

Do podstawowych komponentów systemu zarządzania STRM można zaliczyć:

- **Console** – interfejs i narzędzia zarządzania STRM,
- **Update Daemon** – utrzymuje bazę danych systemu,
- **Event Collector** – pobiera logi z monitorowanych systemów, normalizuje dane i przesyła do Event Processor (przed wysłaniem do Event Processor identyczne zdarzenia są scalane i rejestrowane w systemie identyfikacyjnym STRM); w architekturze rozproszonej STRM komponent Event Collector może działać jako oddzielne Appliance służące do pobierania logów (syslog, snmp, itd.) z innych systemów,
- **Event Processor** – przetwarza dane odbierane z różnych Event Collectors i poddaje je korelacji w oparciu o reguły (także w kontekście analizy behawioralnej), a następnie przesyła dane do Magistrate,
- **Flow Collector** - odczytuje dane z urządzeń sieciowych (NetFlow, J-Flow, S-Flow, itd.),
- **QFlow Collector** - odczytuje dane bezpośrednio z sieci (sniffing) i poddaje je analizie sieciowej i aplikacyjnej,
- **Flow Processor** – tworzy tzw. superflows, czyli flows zagregowane przed tym jak trafiają do Classification Engine,
- **Classification Engine** – analizuje i klasyfikuje flows,
- **Flow Writer** – zapisuje flows oraz profile zasobów (asset profile),
- **Magistrate** – wykonuje przetwarzanie wyższego poziomu, m.in. tworzy perspektywy, raporty, alarmy oraz analizuje ruch sieciowy i zdarzenia bezpieczeństwa, na podstawie których generuje informacje o nadużyciach (offense).

**Offense** to zdarzenie utworzone przez STRM na podstawie wielu źródeł, zwykle zdarzeń z wielu monitorowanych systemów poddanych analizie wraz z wynikami analizy behawioralnej i wskazaniem skanerów zabezpieczeń. Magistrate priorytetyzuje zdarzenia Offense i przydziela im ważność (Magnitude) na podstawie wielu kryteriów (zgodnie z JSL).

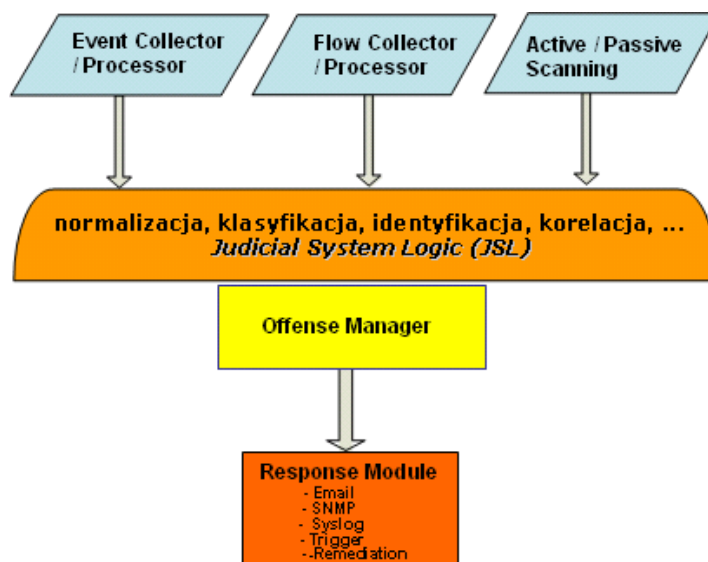
## 2. Zarządzanie logów i obsługa incydentów (SIEM)

Do celów zarządzania zdarzeń (**Log Management**) w STRM utrzymywane jest centralne repozytorium logów. Logi mogą być przeglądane w formie rzeczywistej (raw) lub znormalizowanej. Starsze logi poddawane są kompresji. Informacje składowane w STRM są zabezpieczone kryptograficznie za pomocą sum kontrolnych (także za pomocą "silnej" funkcji SHA-2).

Logi z zewnętrznych systemów są identyfikowane w STRM za pomocą modułów **Device Support Module (DSM)**. STRM automatycznie rozpoznaje urządzenia i systemy wysyłające logi w formacie SYSLOG. Rozpoznane urządzenia i systemy są wyświetlane w zakładce Sensor Devices. Logi przesyłane w formacie innym jak SYSLOG muszą zostać dodane przez administratorów STRM.

Dla administratorów dokonujących obsługi incydentów bezpieczeństwa, przy dużej liczbie generowanych alarmów istotne jest szybkie identyfikowanie najważniejszych zdarzeń. W STRM obowiązują zasady zaczerpnięte z systemu logiki sądowej - **Judicial System Logic (JSL)**. Dla każdego zidentyfikowanego incydentu prezentowana jest jego ważność (*Magnitude*) ustalana na podstawie trzech kryteriów:

1. Wiarygodność (*Credibility*): Jak wiarygodny jest dowód? Jeżeli wielu świadków (źródeł danych) potwierdzi zdarzenie to jego wiarygodność jest wyższa.
2. Istotność (*Relevance*): Ważność zdarzenia (incydentu) zależy od obszaru, gdzie wystąpiło oraz zasobów, których dotyczyło.
3. Surowość (*Severity*): Wielkość zagrożenia zależy m.in. od podatności zasobów na ataki, wartości zasobów, rodzaju ataku, liczby zaatakowanych zasobów.

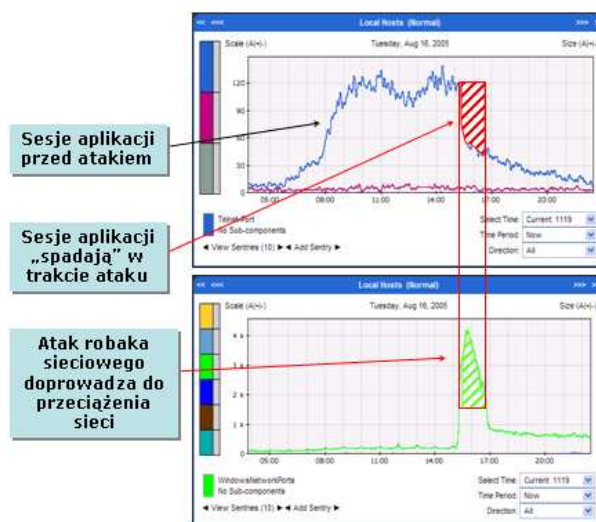


Architektura systemu zarządzania STRM

### 3. Wykrywanie anomalii sieci (NBAD)

Zawarty w Juniper STRM moduł NBAD dokonuje wykrywania anomalii w systemie informatycznym za pomocą analizy behawioralnej. Na bieżąco budowane są profile normalnego stanu i zachowania sieci oraz identyfikowane odchylenia, m.in. zmiany stanu, nagłe zwiększenia lub zmniejszenia natężenia ruchu i przekroczenie wartości progowych. Funkcje NBAD umożliwiają wykrywanie nowych obiektów w systemie informatycznym (hostów, aplikacji, protokołów, itd.) i dzięki temu identyfikowanie zagrożeń i incydentów, m.in. Trojanów nawiązujących połączenia zwrotne z intruzami, wirusów propagujących się przez email oraz serwisów nielegalnie uruchomionych w sieci.

Analiza stanu i zachowania sieci umożliwia także wykrywanie wielu innych niedozwolonych działań jak np. serwerów Web działających jako Proxy, a także partnerów i klientów nadużywających uprawnień (dostęp do obszaru, z którego nie powinni korzystać).



#### Przykład działania NBAD

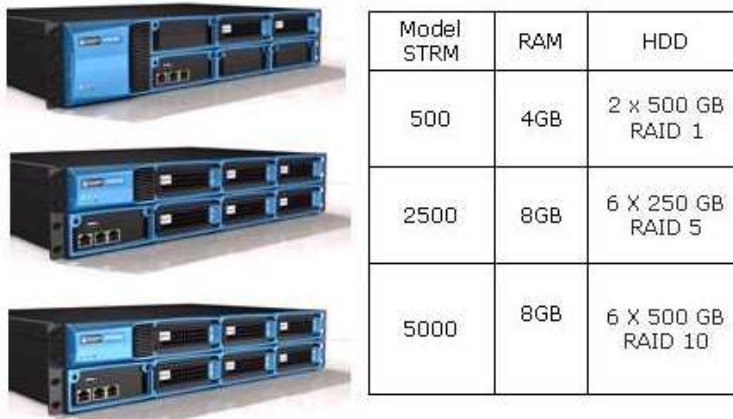
Zawarte w Juniper STRM funkcje NBAD zwiększają możliwości i podwyższają wiarygodność identyfikowanych incydentów bezpieczeństwa SIEM. W tym zakresie można przedstawić wiele przykładów, m.in.:

- analiza ruchu NBAD wykazała, że zaatakowany system tuż po ataku przesłał odpowiedź do sieci zewnętrznej – z dużym prawdopodobieństwem wystąpiło włamanie,
- analiza ruchu NBAD wykazała, że system komunikuje się z serwerem IRC w Internecie, co może wskazywać, że intruz zainstalował w tym systemie IRC Bot,
- analiza ruchu NBAD wykazała, że serwis, który został zaatakowany z dużym prawdopodobieństwem został zablokowany, ponieważ po ataku nie wykazuje aktywności.

Moduł NBAD może zostać także użyty do wykrywania awarii ważnych biznesowo systemów, które powinny być dostępne 24/7, m.in.: zablokowanych/uszkodzonych serwerów i aplikacji, niewykonania operacji backup, urządzeń blokujących ruch.

## 4. Modele i scenariusze wdrożenia STRM

System zarządzania Juniper STRM dostarczany jest w formie „gotowych do użycia” urządzeń Appliance o różnej wydajności i przestrzeni dyskowej – STRM 500, STRM 2500 i STRM 5000.



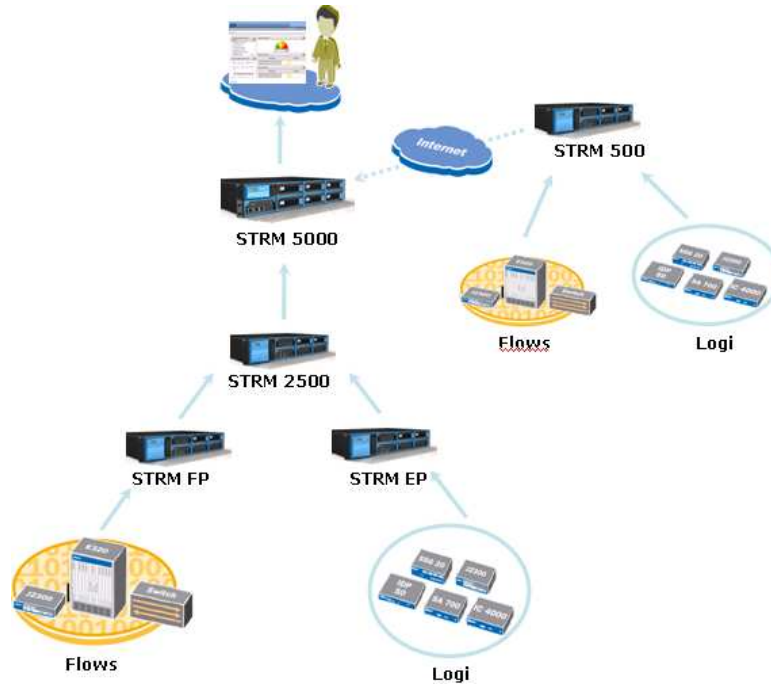
*Modele urządzeń Juniper STRM*

Urządzenie STRM (*chassis*) jest wyposażone w trzy rodzaje wymiennych komponentów sprzętowych (*field-replaceable units, FRU*), które mogą pracować redundancyjnie i być wymieniane w trakcie pracy urządzenia (*hot-swappable*):

- dyski,
- zasilacze,
- wentylatory.

Urządzenia działają na bazie odpowiednio „utwardzonego” systemu operacyjnego klasy Linux (CentOS), umożliwiającego łatwą integrację z zewnętrznymi repozytoriami danych (m.in. iSCSI SAN i NAS).

System zarządzania Juniper STRM może zostać wdrożony w architekturze scentralizowanej (wszystkie funkcje na jednym Appliance) oraz rozproszonej, złożonej z wielu urządzeń. Struktura rozproszona STRM budowana jest w celu zwiększenia wydajności systemu. Także w przypadku rozproszonej struktury STRM zarządzanie całości systemu odbywa się z jednej konsoli.



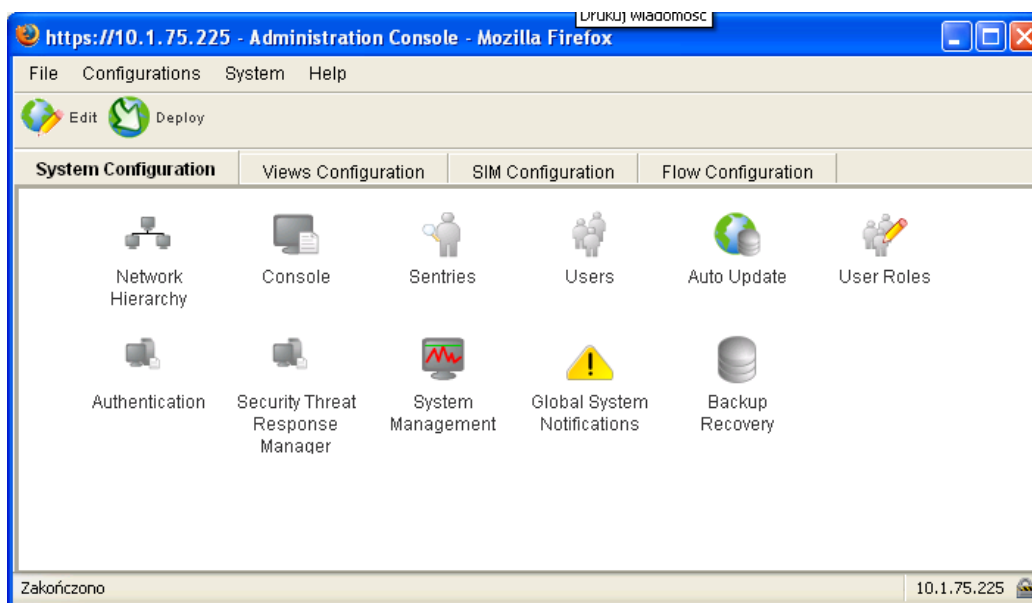
*Przykładowa rozproszona struktura STRM*

## 5. Podstawowa konfiguracja i administracja STRM

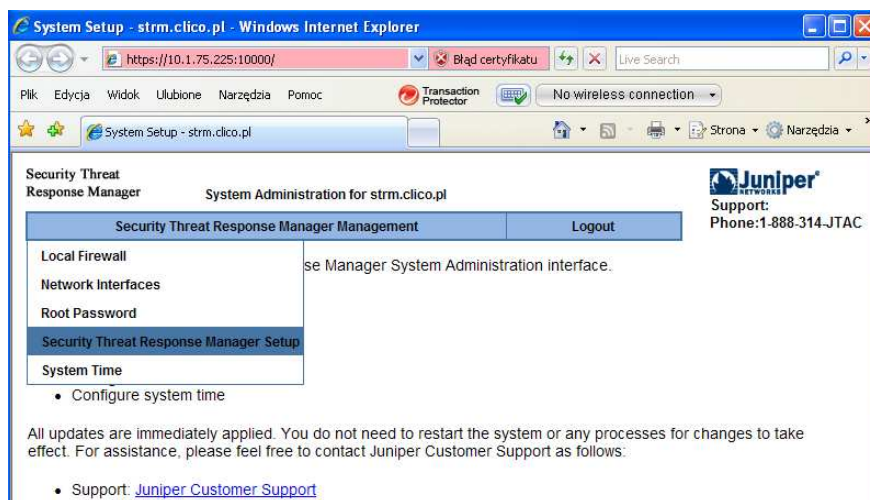
Podstawowy panel konfiguracyjny STRM – CONFIG.



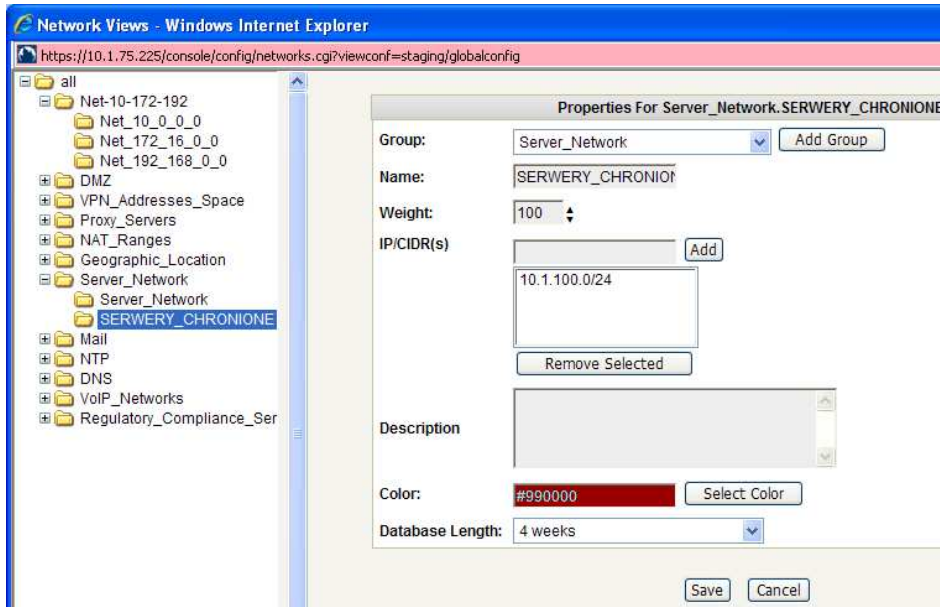
Odbywa się tam konfiguracja podstawowych parametrów systemu STRM (System Configuration), dostrajanie prezentowanych na konsoli informacji (Views Configuration), a także działania modułów SIEM (SIM) i NBAD (Flow).



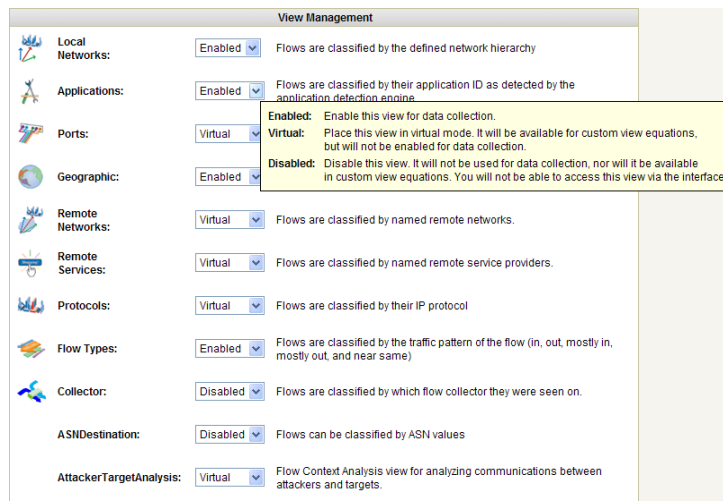
W sekcji System Management dostępna jest konsola do urządzenia



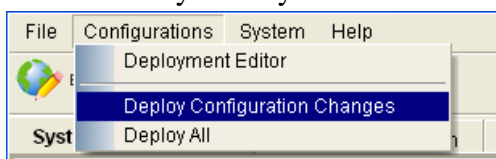
Informacje na temat ruchu w sieci wyświetlane są w odniesieniu do zdefiniowanej hierarchii sieci (**Network Hierarchy**). Hierarchia sieci może zostać zdefiniowana w oparciu o wiele parametrów, w tym geograficznych i funkcjonalnych, np. Sieć wewnętrzna, DMZ, VPN, serwery Proxy, zakresy adresów NAT, podsieci serwerów i VoIP.



Dostrajanie prezentowanych na konsoli informacji o ruchu sieciowym (Views Configuration | Enable/Disable Views).



Zatwierdzamy zmiany.



STRM domyślnie pobiera dane przesyłane za pomocą SYSLOG. Pozostałe protokoły należy w razie potrzeby dodać w konfiguracji.

**Add a protocol configuration**

Configuration Name

Protocol JDBC

JDBC

JDBC:SiteProtector

**JuniperNSM**

LEA

SDEE

SNMPv2

SNMPv3

Wiele urządzeń wysyłających logi poprzez SYSLOG jest w STRM automatycznie rozpoznawanych. W razie potrzeby nowe monitorowane urządzenie należy dodać.

**Edit a sensor device**

Device Name

Sensor Device Type

Protocol Configuration Syslog :: default syslog

Device Description

Device Hostname:IP

Credibility 5

Target Event Collector eventcollector0 :: strm

Coalescing Events Yes

Store Event Payload Yes

Dodajemy monitorowane urządzenia sieciowe, z których będą odczytywane

**Add Flow source**

Build from existing flow source

Flow Source Details

Flow Source Name	<input type="text"/>
Target Flow Collector	<span style="border: 1px solid gray; padding: 2px;">qflow0 :: strm</span>
Flow Source Type	<span style="border: 1px solid gray; padding: 2px;">Flowlog File</span>
<input type="checkbox"/> Enable Asymmetric Flow	<span style="border: 1px solid gray; padding: 2px;">Flowlog File</span>
Flowlog File Configuration	<span style="border: 1px solid gray; padding: 2px;">JFlow</span>
Source File Path	<span style="border: 1px solid gray; padding: 2px;">Netflow v.1/v.5/v.7/v.9</span>
	<span style="border: 1px solid gray; padding: 2px;">Network Interface</span>
	<span style="border: 1px solid gray; padding: 2px;">Packeteer FDR</span>
	<span style="border: 1px solid gray; padding: 2px;">SFlow v.2/v.4/v.5</span>

*Uwaga:* Na monitorowanych urządzeniach i systemach należy skonfigurować wysyłanie logów i flows do systemu STRM.

W razie problemów diagnozujemy poprawność komunikacji sieciowej:

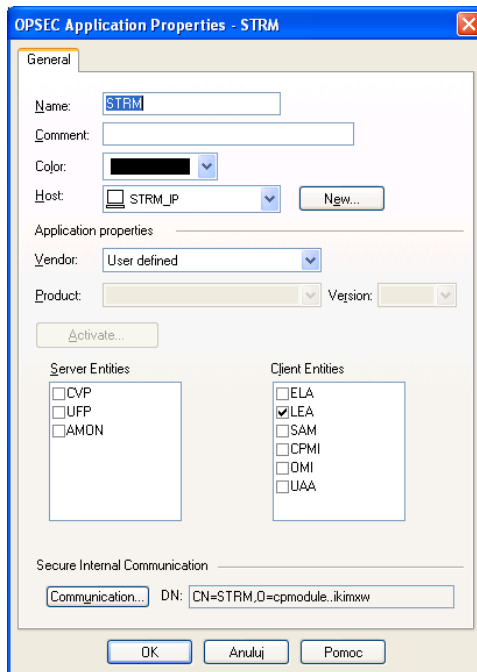
```
[root@strm ~]# ping <IP urządzenia/systemu>
[root@strm ~]# tcpdump -i eth0 host <IP urządzenia/systemu>
```

W razie problemów z odbiorem zdarzeń przez STRM, które nastąpiły po dokonaniu zmian w adresacji monitorowanych systemów zalecany jest restart firewalla:

```
[root@strm ~]# service restart iptables
```

Zgodnie ze specyfiką działania określonych systemów zabezpieczeń dodajemy je do konfiguracji STRM. Poniżej przedstawiony został przykład konfiguracji obsługi zabezpieczeń Check Point.

-- w systemie zarządzania SmartCenter Server (SCS) definiujemy aplikację OPSEC dla STRM i instalujemy politykę



-- w STRM dodajmy nowy protokół OPSEC LEA i nowe urządzenie

OPSEC LEA Configuration Parameters	
<b>Nasz_CP</b>	
Server IP or Hostname	10.1.75.229
Server Port	18184
<input type="checkbox"/> Use Server IP for Event Source	
Statistics Report Interval	600
Authentication Type	sslca
OPSEC Application Object SIC Attribute (SIC Name)	CN=STRM,O=cpmodule,
Log Source SIC Attribute (Entity SIC Name)	cn=cp_mgmt,o=cpmodule,
<input checked="" type="checkbox"/> Specify Certificate	
Certificate Filename	/opt/gradar/conf/opsec,
sensor device	
Device Name	Nasz_CPFW
Sensor Device Type	Check Point FireWall-1
Protocol Configuration	LEA:: Nasz_CP
Device Description	
Device Hostname/IP	10.1.75.229
Credibility	5
Target Event Collector	eventcollector0:: strm
Coalescing Events	Yes
Store Event Payload	Yes
Device Extension	
Extension Use Condition	Parsing Enhancement

W sytuacji gdy komunikacji pomiędzy STRM i Check Point SCS jest kontrolowana przez firewall należy zezwolić STRM dostęp do SCS za pomocą protokołów FW1\_ica\_pull (18210 tcp) oraz FW1\_lea (18184 tcp).

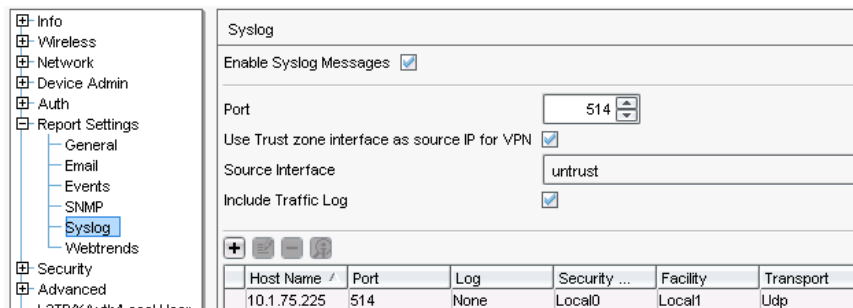
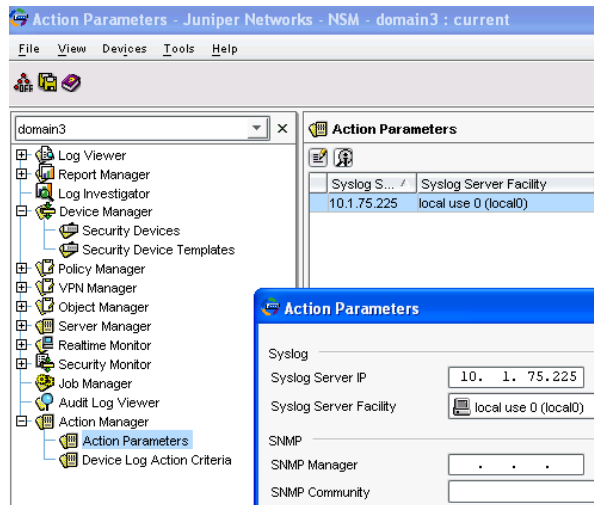
Integracja z systemem zarządzania Juniper NSM wymaga zdefiniowania protokołu Juniper NSM.

Juniper NSM Configuration Parameters	
<b>Nasz_NSM</b>	
IP or Hostname	10.1.75.222
Inbound Port	514
Redirection Listen Port	516
<input type="checkbox"/> Use NSM Address for Event Source	

NSM może zostać w STRM zdefiniowany ręcznie jako monitorowane urządzenie. Po skonfigurowaniu w NSM przesyłania logów do STRM urządzenia zabezpieczeń zarządzane przez NSM (np. IDP, firewall) mogą zostać wykryte przez STRM automatycznie.

Name	Group	Device Type	Enabled	Hostname/IP	Configuration	Target Event Collector	Credibility	Autodiscovered
Linux_dhcp		Linux DHCP Server	true	10.1.75.142	Syslog :: default syslog	eventcollector0 :: strm	5	false
NSM_Serwer		Juniper Networks NetScreen-Security Manager (NSM)	true	10.1.75.222	JuniperNSM :: Nasz_NSM	eventcollector0 :: strm	5	false
Nasz_CPFW		Check Point FireWall-1	true	10.1.75.229	LEA :: Nasz_CP	eventcollector0 :: strm	5	false
NetScreenNSM @ 10.1.75.3		Juniper Networks NetScreen-Security Manager (NSM)	true	10.1.75.3	JuniperNSM :: Nasz_NSM	eventcollector0 :: strm	5	true
Squid_serwer		Squid WebProxy	true	10.1.75.142	Syslog :: default syslog	eventcollector0 :: strm	5	false
Unix_logowanie		Linux login messages	true	10.1.75.142	Syslog :: default syslog	eventcollector0 :: strm	5	false

Logowanie SYSLOG do STRM należy skonfigurować w NSM oraz zarządzanych urządzeniach.



**UWAGA: Szczegółowe wytyczne do integracji STRM z innymi systemami dostępne są w dokumencie „STRM Configuring DSMs”.**

Role i uprawnienia administratorów STRM mogą zostać dostosowane do potrzeb organizacji. Istnieje możliwość ograniczenia poszczególnym administratorom dostępu do ustalonego obszaru systemu informatycznego oraz limitowania operacji w systemie zarządzania STRM. Tożsamość administratorów STRM może być weryfikowana poprzez lokalne konto oraz zewnętrzne systemy uwierzytelniania (m.in. RADIUS, TACACS, LDAP/Active Directory).

### Uprawnienia administratora: System Configuration | User Roles.

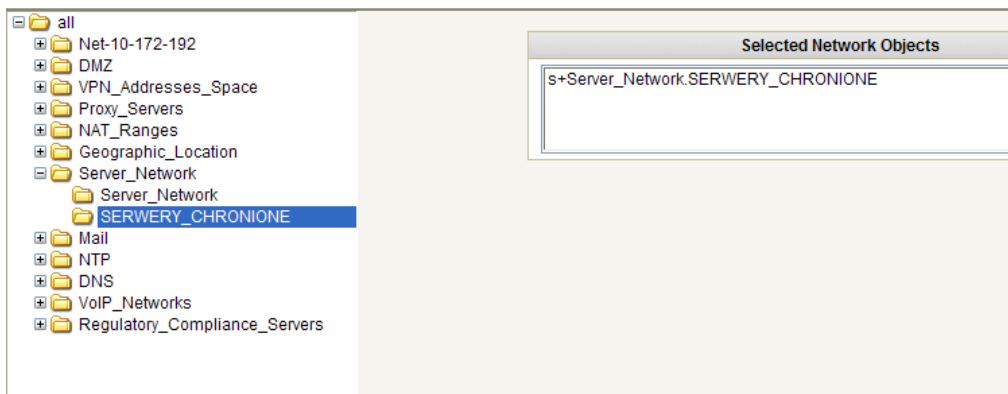
**Manage Role Permissions**

Role Name

Select the permissions associated with this role.

<input type="checkbox"/> <b>Administrator</b>	<input checked="" type="checkbox"/> <b>Offense Management</b>
<input type="checkbox"/> System Administrator	<input checked="" type="checkbox"/> Assign Offenses to Users
<input type="checkbox"/> Administrator Manager	<input checked="" type="checkbox"/> Customized Rule Creation
<input type="checkbox"/> Views Administrator	
<input checked="" type="checkbox"/> <b>Event Viewer</b>	<input checked="" type="checkbox"/> <b>Asset Management</b>
<input checked="" type="checkbox"/> Event Search Restrictions Override	<input checked="" type="checkbox"/> Server Discovery
<input checked="" type="checkbox"/> Customized Rule Creation	<input checked="" type="checkbox"/> View VA Data
	<input checked="" type="checkbox"/> Perform VA Scans
<input checked="" type="checkbox"/> <b>Network Surveillance</b>	<input checked="" type="checkbox"/> <b>Reporting</b>
<input checked="" type="checkbox"/> View Flows	<input checked="" type="checkbox"/> Distribute Reports via Email
<input checked="" type="checkbox"/> View Flow Content	<input checked="" type="checkbox"/> Maintain Templates
<input checked="" type="checkbox"/> View Flows Restrictions Override	
<input checked="" type="checkbox"/> Sentry Modification	

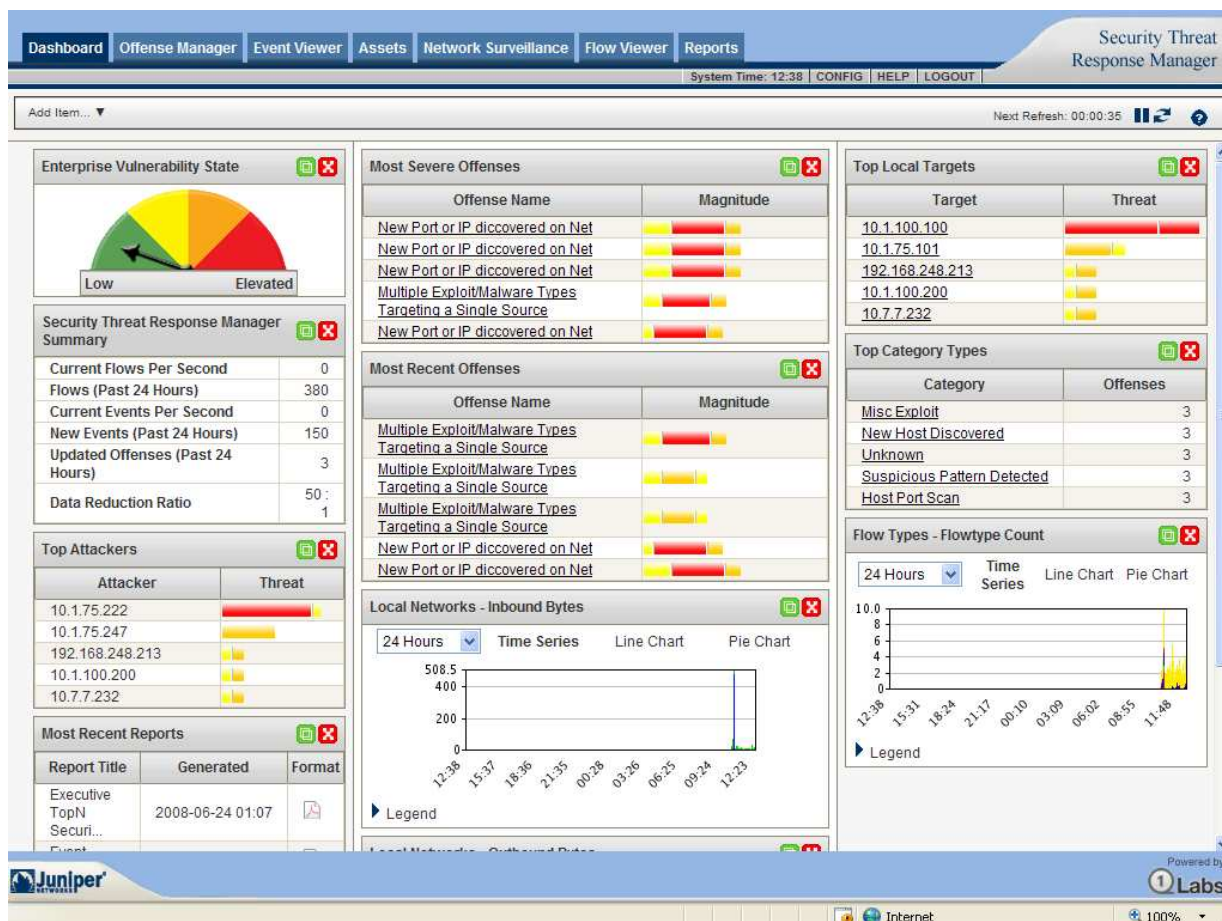
W trakcie definiowania kont administratorów (System Configuration | Users) ustalany jest obszar monitorowania dla określonego administratora.



## 6. Konsola zarządzania Dashboard

Konsola Dashboard stanowi domyślny interfejs STRM uruchamiany po zalogowaniu do systemu. Konsola wyświetla podsumowania oraz rozszerzone informacje o następujących aspektach bezpieczeństwa:

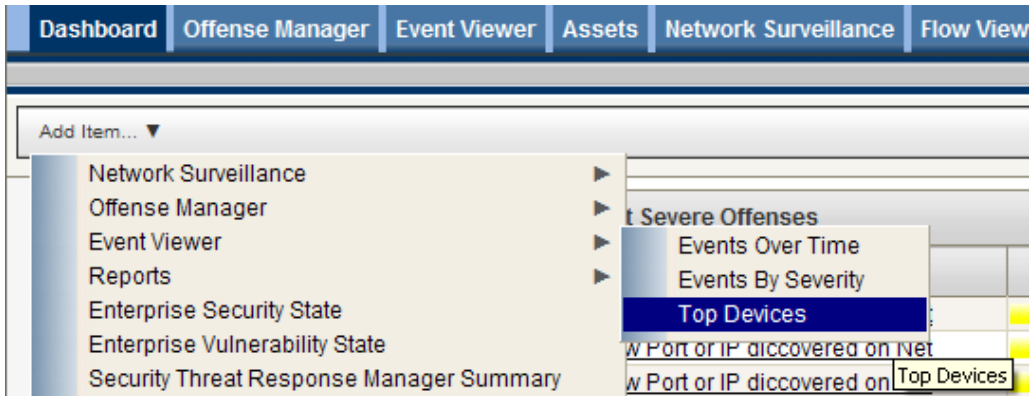
- incydenty bezpieczeństwa w sieci (Offense),
- ogólny stan bezpieczeństwa sieci,
- podgląd stanu i zachowania ruchu sieciowego.



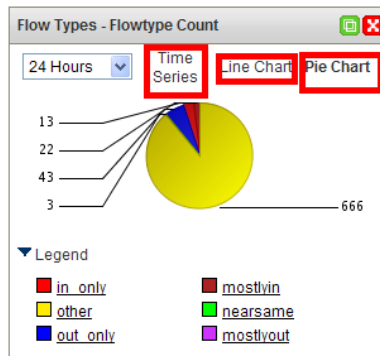
Konsola STRM Dashboard umożliwia:

- monitorowanie liczby wystąpień zdarzeń o określonym poziomie niebezpieczeństwa,
- monitorowanie 10 urządzeń, które w ostatnie 15 minut przesłało do STRM najwięcej zdarzeń,
- monitorowanie incydentów (Offense) przydzielonych dla określonego administratora,
- wyświetlenie ostatnio wygenerowanych raportów,
- wybór przedziału czasowego dla wyświetlanych grafów.

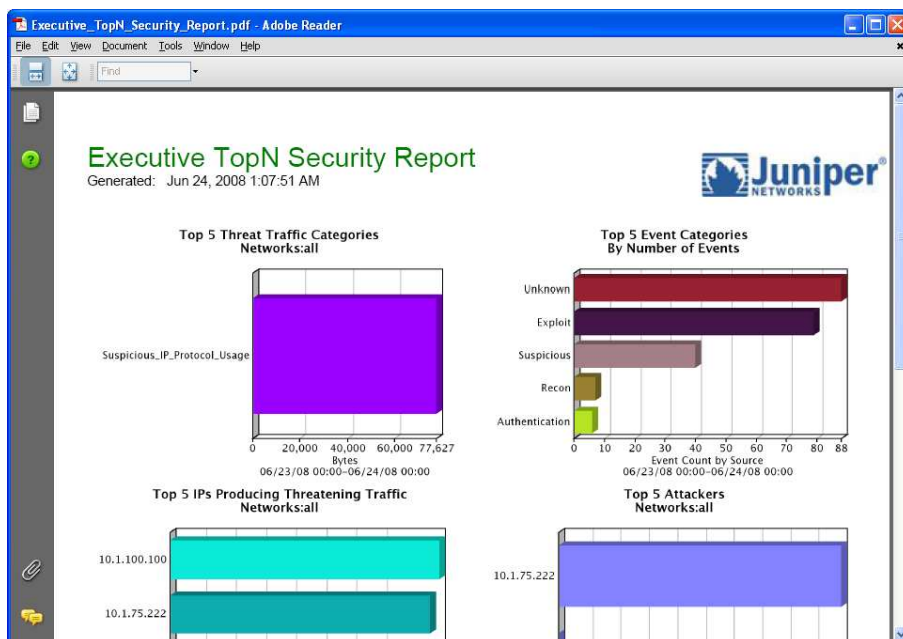
Zawartość Dashboard może być dostrajana do wymagań poszczególnych administratorów.



Konsola umożliwia wyświetlanie danych nt. stanu sieci w różnych formatach (Time Series, Line Chart, Pie Chart).



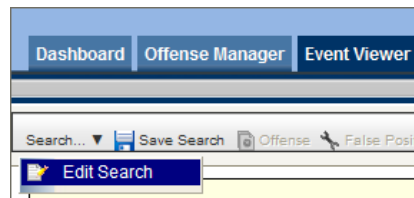
Z poziomu konsoli Dashboard mogą być generowane i zapisywane raporty.



## 7. Przeglądanie zdarzeń Event Viewer

Konsola Event Viewer umożliwia przeglądanie w czasie rzeczywistym zdarzeń (logów) przesyłanych do STRM z możliwością ich selekcji, a także danych historycznych.

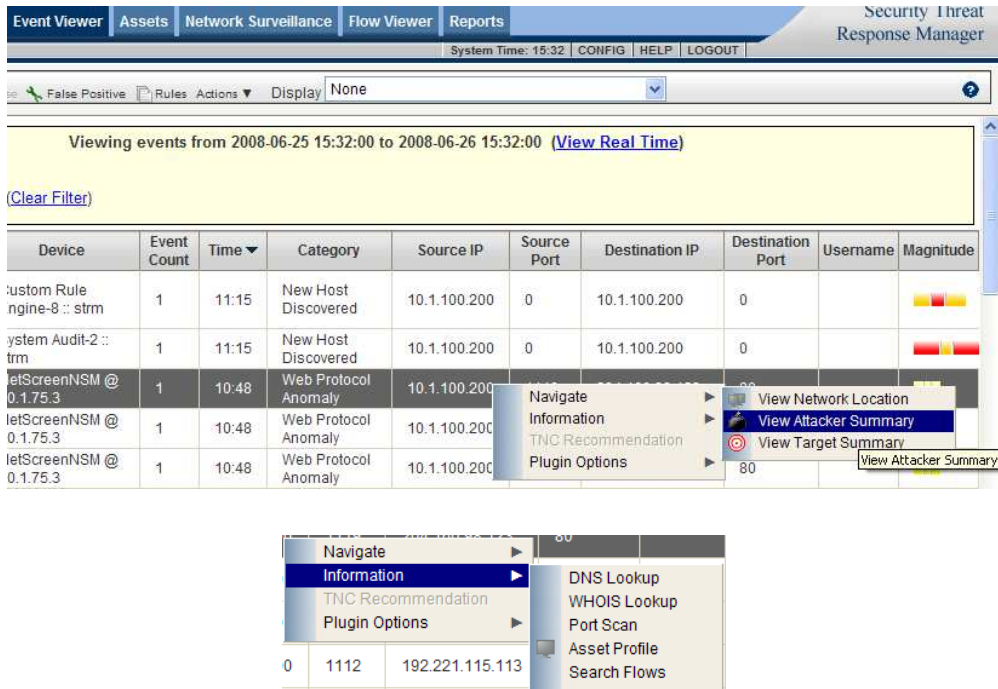
Przeszukiwanie informacji w Event Viewer może odbywać za pomocą różnego rodzaju zapytań i kategorii selekcji. Utworzone w Event Viewer warunki selekcji zdarzeń mogą zostać zapisane i uruchomione w czasie realizacji innych zdań oraz do generowania raportów.



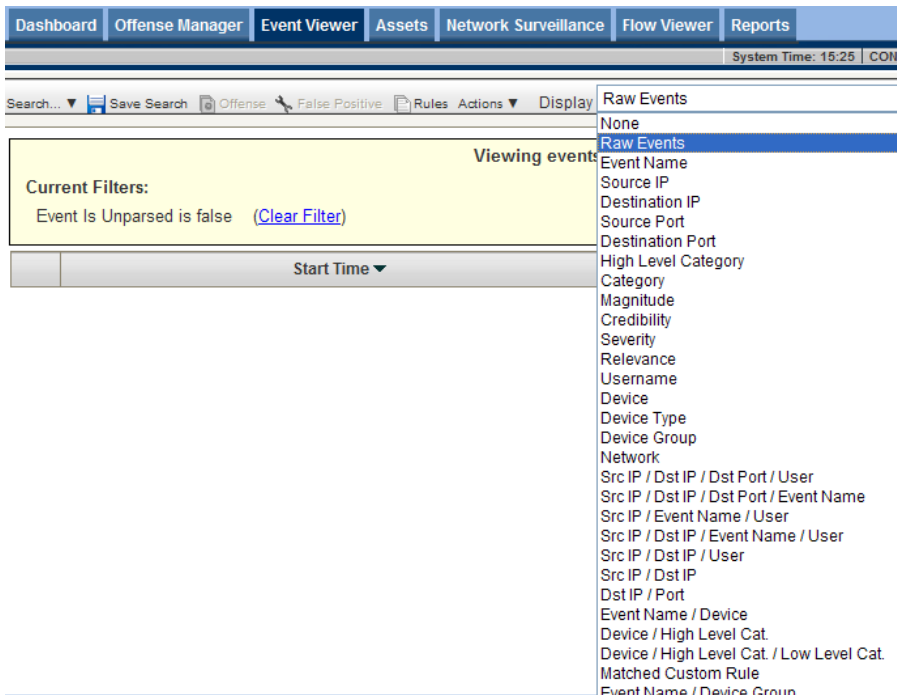
Selekcjonowanie (filtrowanie) informacji może odbywać się z poziomu Event Viewer.

Event Name	Device	Event Count	Time ▲	Category	Source IP	S
HTTP Info: URL Access	NetScreenNSM @ 10.1.75.3	1	10:38	Web Protocol Anomaly	10.1.75.111	1
HTTP Info: URL Access	NetScreenNSM @ 10.1.75.3	1	10:38	Web Protocol Anomaly	10.1.75.111	1
HTTP Info: URL Access	NetScreenNSM @ 10.1.75.3	1	10:38	Web Protocol Anomaly	10.1.75.111	1
HTTP Info: URL Access	NetScreenNSM @ 10.1.75.3	1	10:39	Web Protocol Anomaly	10.1.75.111	1

Administrator STRM ma do dyspozycji dodatkowe informacje o zdarzeniu, wyświetlane bezpośrednio z Event Viewer.



Przeglądane logów w Event Viewer może odbywać się dla zdarzeń zagregowanych (pogrupowanych) względem różnych atrybutów (np. adresy IP generujące najwięcej incydentów). Domyślnie informacje wyświetlane są w postaci znormalizowanej. Można jednak przeglądać dane w formie rzeczywistej (row) lub zagregowanej – opcje *Display*.



## 8. Zarządzanie incydentów Offense Manager

Konsola Offense Manager przedstawia zidentyfikowane naruszenia bezpieczeństwa w sieci z możliwością ich analizy.

Id	Description	Attacker/Src	Magnitude	Target(s)/Dest	Attacker Net
42	New Port or IP discovered on Net	10.1.75.246	9	10.1.75.246	Net_10_0_0_0
41	New Port or IP discovered on Net	10.7.7.232	9	10.7.7.232	Net_10_0_0_0
40	New Port or IP discovered on Net	10.1.100.200	9	10.1.100.200	Net_10_0_0_0
39	New Port or IP discovered on Net	192.168.248.213	9	192.168.248.213	Net_192_168_0_0
3	Multiple Exploit/Malware Types Targeting a Single Source	10.1.75.222	9	Multiple (2)	Net_10_0_0_0

Relevance 1, Severity 9, Credibility 4, Magnitude 4

Offense Manager umożliwia wyeksportowanie danych o intruzach i celach ataków do formatu XML lub CSV (np. do wygenerowania raportu), a także przypisanie zdarzenia do obsługi przez określonego administratora STRM.

Id	Description	Attacker/Src	Magnitude	Target(s)/Dest
42	New Port or IP discovered on Net	10.1.75.246	9	10.1.75.246
41	New Port or IP discovered on Net	10.7.7.232	9	10.7.7.232
40	New Port or IP discovered on Net	10.1.100.200	9	10.1.100.200
39	New Port or IP discovered on Net	192.168.248.213	9	192.168.248.213
3	Multiple Exploit/Malware Types Targeting a Single Source	10.1.75.222	9	Multiple (2)

Assign this offense to a user

Naruszenie bezpieczeństwa w STRM zwykle identyfikowane są na podstawie wielu źródeł. Konsola Offense Manager umożliwia szczegółową analizę zdarzeń i warunków ich wystąpienia.

**Offense 3**

Magnitude	All categories of this offense		Relevance	1	Severity	9	Credibility	4
Description	Multiple Exploit/Malware Types Targeting a Single Source		Event count	461 events in 14 categories				
Attacker:Src	10.1.75.222		Start	2008-06-16 14:10:22				
Target(s):Dest	10.1.100.100 Remote (1)		Duration	7d 22h 11m 47s				
Network(s)	Multiple (2)		Assigned to	Not assigned				
Notes								

**List of Event Categories**

Name	Magnitude	Local Target Count	Events	Last Event
UDP Exploit	■■■■	1	17	06-24 12:11:17
RPC Exploit	■■■■	1	50	06-24 12:19:50
Potential FTP Vulnerability	■■■■	1	46	06-24 12:20:01
Samba Exploit	■■■■	1	15	06-24 12:19:51
Host Login Failed	■■■■	1	24	06-24 12:20:01
Misc Exploit	■■■■	1	33	06-24 12:19:51
FTP Exploit	■■■■	1	67	06-24 12:19:50
Compliance: Botnet Detected	■■■■	1	76	06-24 12:20:01

STRM posiada zestaw predefiniowanych reguł korelacji zdarzeń. Dzięki temu na podstawie wielu pojemnych zdarzeń potrafi w sposób wiarygodnych wskazać naruszenia bezpieczeństwa.

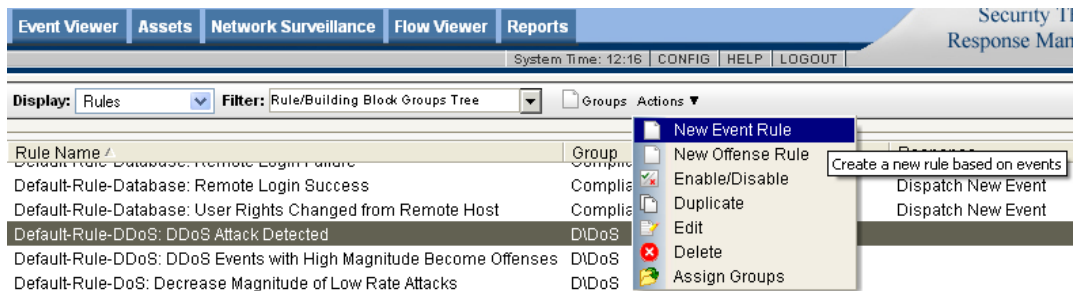
**Rules**

Rule Name	Group	Rule Type	Enabled	Response
Default-Rule-Authentication: Login Failures Across Multiple Hosts	Authentication	EVENT	true	Dispatch New Event
Default-Rule-Authentication: Login Failures Followed By Success	Authentication	EVENT	true	Dispatch New Event
Default-Rule-Authentication: Login Successful After Scan Attempt	Authentication	EVENT	true	Dispatch New Event
Default-Rule-Authentication: Multiple VoIP Login Failures	Authentication	EVENT	true	Dispatch New Event
Default-Rule-Authentication: Repeated Login Failures, Single Host	Authentication	EVENT	true	Dispatch New Event
Default-Rule-Botnet: Potential Botnet Connection (DNS)	Botnet, Exploit	EVENT	false	Dispatch New Event
Default-Rule-Botnet: Potential Botnet Connection (IRC)	Botnet	EVENT	true	Dispatch New Event
Default-Rule-Botnet: Potential Botnet Events Become Offenses	Botnet	EVENT	true	
Default-Rule-Compliance: Compliance Events Become Offenses	Compliance	EVENT	false	
Default-Rule-Compliance: Excessive Failed Logins to Compliance IS	Compliance	EVENT	false	Dispatch New Event
Default-Rule-Database: Attempted Configuration Modification by a remote I	Compliance, I	EVENT	true	Dispatch New Event

**Rule**

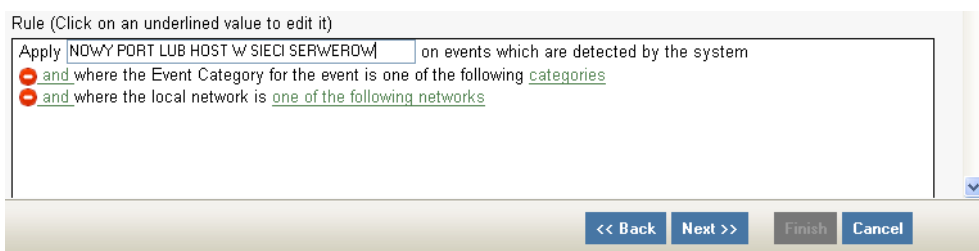
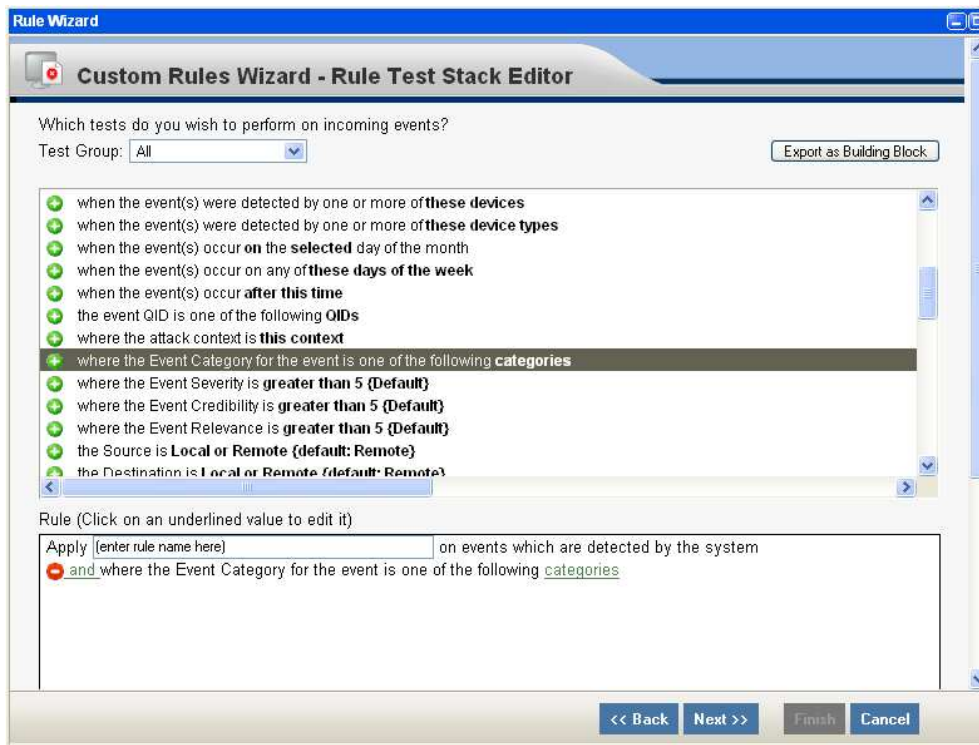
Apply Default-Rule-Authentication: Multiple VoIP Login Failures on events which are detected by the system and when we see an event match any of the following Default-BB-HostDefinition: VoIP PBX Server and when we see any of these Default-BB-CategoryDefinition: VoIP Authentication Failure Events with the same source IP more than 3 times, across exactly 1 destination IP(s) within 30 seconds

Administratorzy STRM mogą w razie potrzeby definiować własne reguły korelacji zdarzeń i obsługi naruszeń bezpieczeństwa. Reguły mogą operować na zdarzeniach (New Event Rule) oraz naruszeniach (New Offense Rule).



Odbywa się to za pomocą kreatora reguł **Rule Wizard**. Poniżej przedstawiony został proces tworzenia reguły korelacji zdarzeń. Odbywa się w to w następującej kolejności.

1. Wybór testów wykonywanych przez STRM na odbieranych zdarzeniach (zasad identyfikacji).



Uwaga: Testy mogą być dodawane w relacji iloczynu logicznego 'and' oraz zaprzeczenia 'and NOT'. W razie potrzeby zdefiniowana relacji logicznej OR należy użyć testu typu *Multi-Rule Event Function* i wskazać poszczególne testy (reguły) z opcją 'any'.

Przykład poniżej.

Rule (Click on an underlined value to edit it)

Apply Wykrywanie skanowania portów TCP lub UDP on events which are detected by the system

and when we see an event match any of the following Default-Rule-Recon: Remote TCP Scanner, Default-Rule-Recon: Remote UDP Scanner

<< Back Next >> Finish Cancel

## 2. Dostrajamy parametry testów.

Select a category and click 'Add'

VIS Host Discovery  
 VIS Host Discovery.Bulk Host Discovered  
 VIS Host Discovery.New Host Discovered  
 VIS Host Discovery.New OS Discovered  
 VIS Host Discovery.New Port Discovered  
 VIS Host Discovery.New Vuln Discovered

Add +

Selected Items

VIS Host Discovery.New Port Discovered  
 VIS Host Discovery.New Host Discovered

Remove -

Submit Cancel

Select a desired network and click 'Add'

Net-10-172-192  
 DMZ  
 VPN\_Addresses\_Space  
 Proxy\_Servers  
 NAT\_Ranges  
 Geographic\_Location  
 Server\_Network
 

- Server\_Network
- SERWERY\_CHRONIONE

 Mail

Add +

Selected Items

Server\_Network.SERWERY\_CHRONIONE

Remove -

Submit Cancel

Rule (Click on an underlined value to edit it)

Apply NOWY PORT LUB HOST W SIECI SERWEROW on events which are detected by the system

and where the Event Category for the event is one of the following VIS Host Discovery.New Host Discovered, VIS Host Discovery.New Port Discovered

and where the local network is Server\_Network.SERWERY\_CHRONIONE

<< Back Next >> Finish Cancel

Zdefiniowane testy mogą zostać zapisane i użyte do tworzenia kolejnych reguł.

Export as Building Block

### 3. Konfigurujemy zasady obsługi zdarzeń i zatwierdzamy utworzoną regułę.

W sekcji **Rule Action** możemy ustawić parametry ważności zdarzenia (*Severity, Credibility, Relevance*), przesłać zdarzenie do dalszej analizy i korelacji z innymi zdarzeniami (*Ensure the detected event is part of an offense*) lub przeznaczyć zdarzenie tylko do archiwizacji (*Drop the detected event*).

W sekcji **Rule Response** wybieramy opcję **Dispatch New Events** tak, aby informacja o nowym zdarzeniu (incydencie) była wyświetlana w konsoli STRM oraz wybieramy kategorię **User Defined**. Dodatkowo zaznaczamy opcję **Ensure the dispatched event is part of an offense** tak, aby przesłać zdarzenie do dalszej analizy i korelacji z innymi zdarzeniami (do Magistrate).

Nową regułę aktywujemy.

## 9. Analiza bezpieczeństwa chronionych zasobów (Assets)

Skuteczna obsługa incydentów koncentruje się na identyfikacji ich sprawców (użytkowników, hackerów, złośliwego kodu). W systemie STRM jest utrzymywana i na bieżąco aktualizowana baza **Asset Profile**, która umożliwia przeszukiwanie zgromadzonych informacji o zasobach systemów informatycznych zgodnie z wieloma kryteriami. Zdarzenia analizowane przez STRM są powiązane z nazwami użytkowników, nazwami komputerów oraz adresami IP/MAC. Wiarygodność incydentów jest ustalana na podstawie wielu źródeł – logów różnych systemów, ruchu w sieci oraz skanerów zabezpieczeń, itd.

The screenshot displays the 'Asset Profile' configuration page in the STRM console. The form contains the following fields and values:

Name	Komputer serwisantow		
Description			
IP Address	10.1.75.222	VA Risk Level	3
Operating System		How Threatening	10
Host Name (DNS Name)	10.1.75.222	How Threatened	0
Asset Weight	0 - Not Important		
MAC		Host Name	
Machine Name		User Group	
User Name			
Extra Data			

Below the form is a table for port information:

Port	OSVDB ID	Name	Description	Risk / Severity	Last Seen	First Seen
No port information is available for this IP address. The selected IP address may not have been scanned and/or has not generated any traffic.						

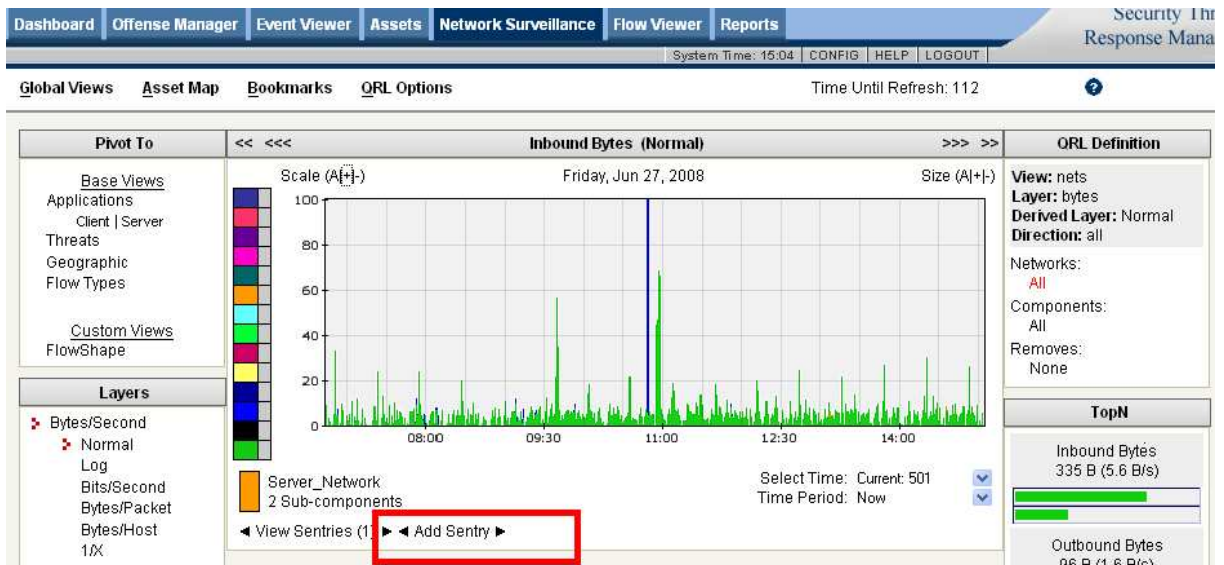
Dane określające tożsamość użytkowników mogą zostać ustalone na podstawie wielu różnych systemów, m.in. Juniper Steel Belted Radius, Juniper Infranet Controller, Cisco Secure Access Control Server, Linux Authentication Server, ArrayNetworks ArrayVPN, Check Point SmartCenter/Provider-1, Cisco VpnConcentrator, F5 BigIP, Juniper NetScreen/SSG, Juniper SA, itd.

## 10. Analiza stanu sieci (Flow Viewer, Network Surveillance)

Konsola Flow Viewer umożliwia monitorowanie i analizowanie w czasie rzeczywistym informacji na temat ruchu sieciowego (Flow) oraz wykonywanie różnego rodzaju przeszukiwania danych. Flow rozumiany jest jako sesja komunikacyjna pomiędzy dwoma hostami w sieci. Informacje mogą być przeszukiwane i w razie potrzeby agregowane. Na podstawie zapisanych warunków selekcji mogą być generowane raporty. Dane o ruchu sieciowym mogą zostać wyeksportowane do formatów XML lub CSV.

Flow Type	First Packet Time	Last Packet Time	Source IP	Source Port	Destination IP	Destination Port	Source Bytes	Destination Bytes	Total Bytes	Source Packets	Destination Packets	Total Packets	Protocol
	2008-06-27 14:53:53	14:53	10.1.100.200	3235	192.168.248.213	914	48	0	48	1	0	1	TCP.tcp_ip
	2008-06-27 14:53:24	14:53	10.1.100.101	138	10.1.100.255							1	UDP.udp_i
	2008-06-27	14:53	10.1.75.111	138	10.1.75.255	138	229	0	229	1	0	1	UDP.udp_o

Konsola Network Surveillance przedstawia bieżące obciążenie sieci różnego rodzaju ruchem z możliwością definiowania zdarzeń typu Sentry (np. wykrywania i alarmowania w sytuacjach wyjątkowych).



## 11. Integracja STRM z Juniper NSM i Profiler

System zarządzania STRM posiada możliwość integracji z Juniper NSM w zakresie bezpośredniego korzystania z utrzymywanej przez NSM bazy danych Profiler. Znajdują się tam informacje na temat stanu chronionych zasobów IT, uzyskane w wyniku pasywnego skanowania ruchu przez urządzenia zabezpieczeń Juniper IDP.

Administrator STRM z poziomu konsoli Event Viewer może odczytać szczegółowe informacje dotyczące określonego systemu (np. komputera intruza).

Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magn
New Host Discovered	10.1.100.200	0	10.1.100.200	0		
New Host Discovered	10.1.100.200	0	10.1.100.200	0		
Web Protocol Anomaly	10.1.100.200	4444	10.1.100.200	80		
Web Protocol Anomaly	10.1.100.200			80		

Juniper IDP Profiler Query Results for: 10.1.100.200

Host Information for: 10.1.100.200

IP Address	MAC Address	OS
10.1.100.200	00:05:85:cf:46:40	Windows:2000 SP4, XP SP1

Service Information for: 10.1.100.200

Port	Protocol	Service	Value
21	TCP	FTP Banner	3Com 3C Daemon FTP Server Version 2.0
21	TCP	FTP Request	QUIT
21	TCP	FTP Command	QUIT
21	TCP	FTP Banner	sp Microsoft FTP Service (Version 5.0).
21	TCP	FTP Request	USER nessus10085388312941350
21	TCP	FTP Username	nessus10085388312941350

STRM należy odpowiednio skonfigurować w zakresie integracji z systemem zarządzania Juniper NSM/Profiler.

1. W konsoli STRM dodajemy skaner dla Juniper IDP Profiler.

2. Na urządzeniu STRM w katalogu '/' uruchamiamy polecenie:

```
[root@strm conf]# tar -xzf profiler-rightclick.tgz
```

3. Edytujemy plik `/opt/qradar/conf/JuniperProfilerRightClick.properties` gdzie podajemy adres IP NSM oraz id i hasło dostępu do bazy danych NSM.

4. Otwieramy plik `/opt/qradar/conf/ip_context_menu.xml` i jeżeli nie istnieje to dodajemy linię:

```
<menuEntry name="Juniper IDP Profile" url="/console/JuniperProfilerRightClick.jsp?hostIp=%IP%" />
```

pomiędzy znacznikami `<contextMenu>` i `</contextMenu>`.

5. Linki symboliczne powinny być ustawione następująco:

```
[root@strm conf]# ls -al geo*
lrwxrwxrwx 1 root root 32 Jul 15 12:50 geographic.classify.conf ->
geographic.classify.country.conf
-rw-rw-r-- 1 nobody nobody 10793198 Jul 15 10:29 geographic.classify.continent.conf
-rw-rw-r-- 1 nobody nobody 9751302 Jul 15 10:29 geographic.classify.country.conf
lrwxrwxrwx 1 root root 23 Jul 15 12:50 geographic.conf -> geographic.country.conf
-rw-rw-r-- 1 nobody nobody 507 Jul 15 10:29 geographic.continent.conf
-rw-rw-r-- 1 nobody nobody 9163 Jul 15 10:29 geographic.country.conf
```

Jeżeli jest inaczej należy je zmodyfikować i zrestartować STRM.

```
[root@strm conf]# rm geographic.classify.conf
[root@strm conf]# rm geographic.conf
[root@strm conf]# ln -s geographic.classify.country.conf geographic.classify.conf
[root@strm conf]# ln -s geographic.country.conf geographic.conf
```

STRM można zrestartować poleceniem 'reboot' lub sekwencją poleceń:

```
# service hostcontext stop
# service tomcat stop
# service imq stop
# service postgresql restart
# service imq start
# service tomcat start
# service hostcontext start
```

## 12. Tworzenie statystyk i raportów

STRM oferuje wiele typów raportów tworzonych zgodnie z kryteriami ustalonymi przez administratorów oraz raportów predefiniowanych (ponad 200), w tym na zgodność ze standardami (m.in. PCI, SOX, FISMA, GLBA, HIPAA).

Report Title	Group	Schedule	Generated	Owner	Template Author	Format
Executive TopN Security Report	Network Management	Daily	2008-06-27 01:07	admin	admin	[Icon]
Event Distribution	Executive	Daily	2008-06-27 01:07	admin	admin	[Icon]
Daily Top Targeted Assets by VA Risk	Network Management	Daily	2008-06-27 01:06	admin	admin	[Icon]
Daily Top Security and Policy Offenses	Network Management	Daily	2008-06-27 01:06	admin	admin	[Icon]
Daily Security Event Summary	Executive	Daily	2008-06-27 01:06	admin	admin	[Icon]
Daily Offense Manager Summary	Executive	Daily	2008-06-27 01:05	admin	admin	[Icon]
Daily Network Throughput Summary	Executive	Daily	2008-06-27 01:05	admin	admin	[Icon]
Daily Executive Traffic Policy Summary	Executive	Daily	2008-06-27 01:04	admin	admin	[Icon]
Daily Executive Threat Summary	Executive	Daily	2008-06-27 01:04	admin	admin	[Icon]
Daily Executive Security Overview	Executive	Daily	2008-06-27 01:03	admin	admin	[Icon]
Daily Executive Policy Overview	Executive	Daily	2008-06-27 01:03	admin	admin	[Icon]
Daily Executive Application Usage Summary	Executive	Daily	2008-06-27 01:02	admin	admin	[Icon]
Daily Enterprise Network Usage Summary	Executive	Daily	2008-06-27 01:02	admin	admin	[Icon]
Daily Delta Network Usage Summary	Executive	Daily	2008-06-27 01:01	admin	admin	[Icon]
Daily Attacker and Target Summary	Executive	Daily	2008-06-27 01:01	admin	admin	[Icon]
Daily At-A-Glance Network Health Summary	Executive	Daily	2008-06-27 01:01	admin	admin	[Icon]

Page: 1 Go << 1 | 2 | 3 | ... | 14 >>

Do dyspozycji administratorów STRM dostępny jest intuicyjny kreator raportów. Raporty mogą być tworzone w wielu formatach (m.in. PDF, HTML, RTF, CVS, XML).

