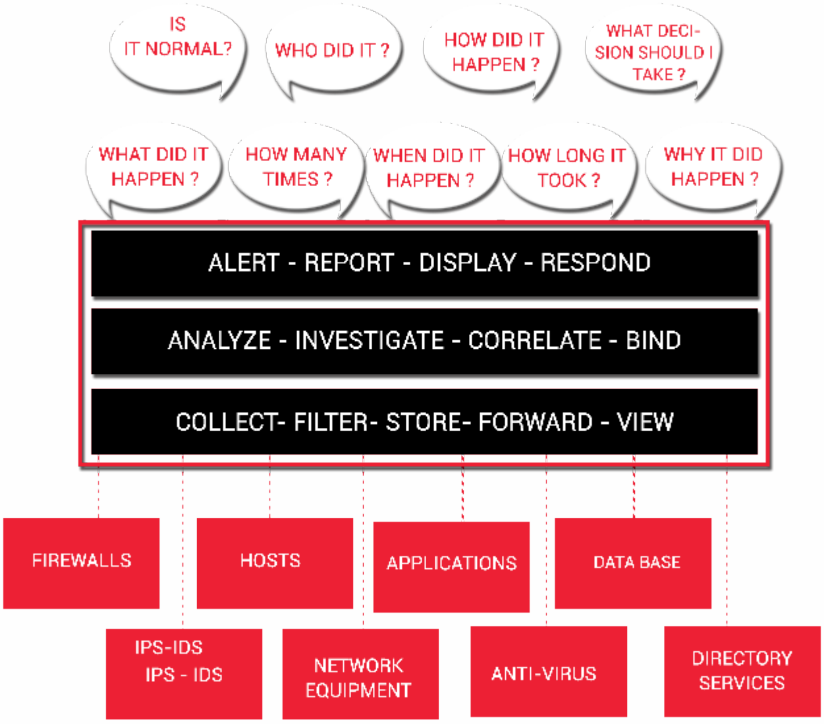
SECNOLOGY

THE GLOBAL EVENT MANAGER

TURN DATA INTO ACTIONS

When data is available and reachable, it has to be processed and decrypted using multiple heterogeneous tools, if these are available. Each of these tools requires a specific skill set and time. Each device often has its own monitoring tool, its own way of processing data, and its own management needs and restrictions.

For events and traces, the situation is even more complex. These devices generate events with their own proprietary format. These event formats are structured or unstructured with their own specific meaning. The complexity increases when the same device can generate different event formats based on the way it is configured by the administrator.
From the user's perspective, the needs are quite clear and the queries addressed to these devices are simple and precise. In spite of that, it is challenging to get a single standard view of all the information. Addressing this challenge is SECNOLOGY's main objective and principal mission.



A single tool with a user friendly interface, a single homogeneous and standard view for all your data, regardless of their source, their location, their format, their size, in real-time or on-demand and correlated if needed, that is SECNOLOGY.

SECNOLOGY is a turnkey, user friendly, universal event management and correlation solution dedicated to Big Data Mining with breakthrough technology and a unique architecture. With SECNOLOGY, users are able to process years of data and billions of records a day as well as access to all their information instantly.
The concept, which makes SECNOLOGY unique, is due to two factors:

1. Architecture in this field is usually based on Database standards (Recognition of the fact that machine generated data management is very different from human generated data management
2. Introduction of the Big Data Mining concept based on a very clear knowledge of end-user needs and objectives in managing machine generated data on a day-to-day basis

Architecture in this field is usually based on Database standards (relational or object oriented).These standards are ideal and mandatory for structured and dynamic data processing such as stock management, flight booking, ticket reservation, etc. where the Data is changing continuously. However, with machine-generated data, we are talking about traces. Traces are historical and therefore static and permanent.
They never change and we must prevent any change for this type of data. Another approach is needed to manage this type of data. . This is the reason why SECNOLOGY spent 7 years developing its patented turbo indexing methodology (STIM). Using STIM, SECNOLOGY does not require a database, a dedicated server, web servers, or development toolkits, and you can get everything you need out of your data.

However, with machine-generated data, we are talking about traces. Traces are historical and therefore static and permanent. They never change and we must prevent any change for this type of data. Another approach is needed to manage this type of data. This is the reason why SECNOLOGY spent 7 years developing its patented turbo indexing methodology (STIM). Using STIM, SECNOLOGY does not require a database, a dedicated server, web servers, or development toolkits, and you can get everything you need out of your data.

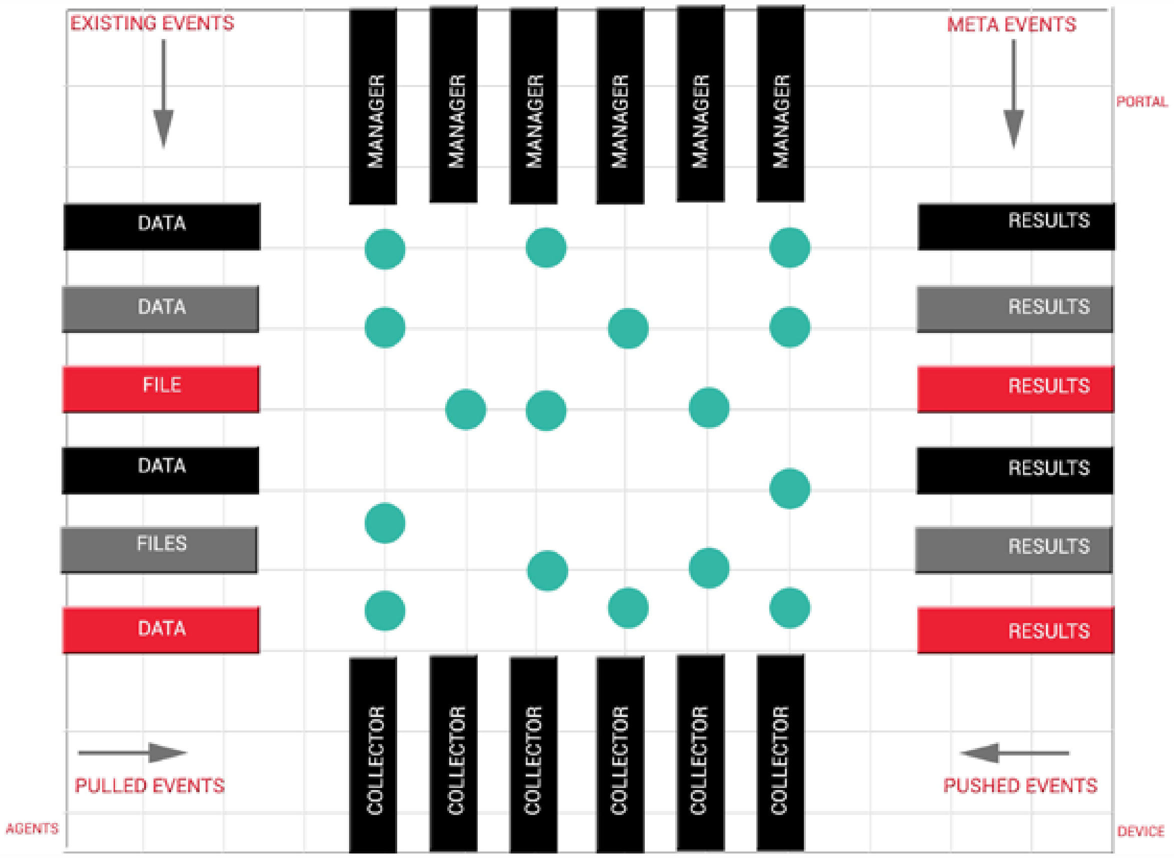
Global Event Consolidation Features

SECNOLOGY may be a TCP or UDP SYSLOG Server, but it is much more than that. SECNOLOGY collects real-time events from anywhere and from many devices simultaneously using UDP, TCP, SSL, SNMP, POP3, CIDEE, SDEE, NetFlow, jFlow, sFlow, MS-EVENTS, or LEA OPSEC protocols.

SECNOLOGY's SECagent actively captures event data from sources that are unable to send, which ensures that real-time analysis is complete and comprehensive. SECagent will fetch, watch, pull, and send this data to SECNOLOGY on the fly. SECagent is able to watch file systems, Windows events, data files, folders, registry keys and Active Directory or LDAP events. This includes the ability to extract and audit user privileges and track user activity in real-time.

With SECNOLOGY, manage all types of events whether they are real-time or historical. Data to process may arrive on the fly or may already reside somewhere on the network in flat files or in existing databases.

Performance by design



SECNOLOGY enables you to collect a large number of events directly from your devices, registry or files in real time, on event or on demand. Store data centrally and/or remotely, archive and secure the data according to policy, and more generally automatically manage the whole data life cycle, including availability, accessibility, integrity, confidentiality, segregation, period retention and purging, in accordance with your policies.

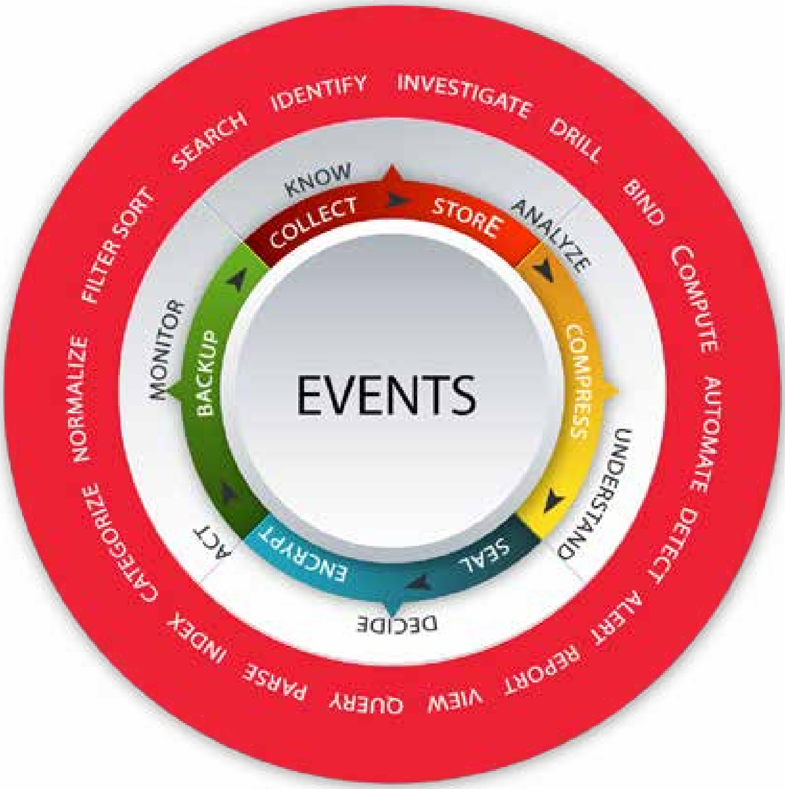
TURN DATA INTO ACTIONS

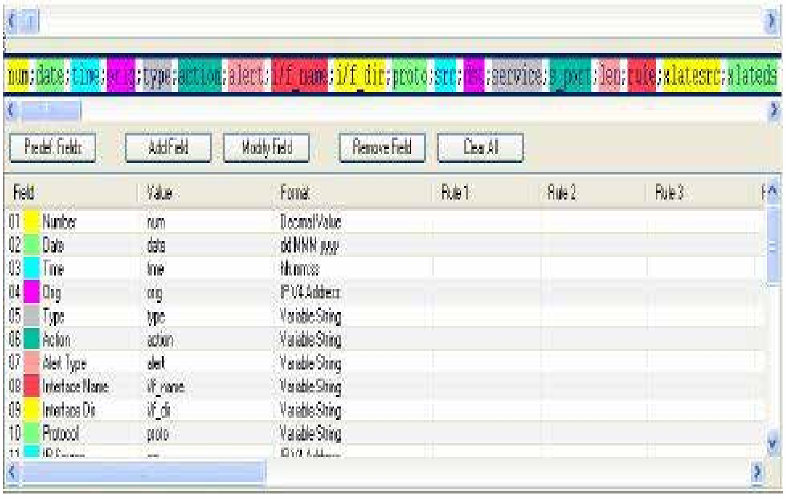
TURN DATA EVENTS INTO KNOWLEDGE

TURN KNOWLEDGE INTO ACTIONS

Use SECNOLOGY to:

- Search and explore data and events
- Parse events and traces
- Filter data events
- Segregate data events
- Normalize data events
- Categorize data events
- Detect anomalies
- Enrich data events
- Correlate multiple data events from different sources
- Evaluate triggers and measure thresholds
- Compare different metrics
- Process data events
- Process jobs and alerts
- Manage the data event life cycle
- Create graphs and charts
- Provide dashboards
- Investigate after an incident
- Perform in real-time
- Generate reports in real-time
- Monitor in real-time the global environment
- Log all the traces of all actions made in the environment




num;date;time;orig;type;action;alert;i/f_name;i/f_dir;proto;src;dst;service;s_port;len;rule;xlatesrc;xlateds
Predef. Fields
Add Field
Modify Field
Remove Field
Clear All

Field		Value	Format	Rule 1	Rule 2	Rule 3
01	Number	num	Decimal Value			
02	Date	date	dd MMM yyyy			
03	Time	time	hh:mm:ss			
04	Orig	orig	IPV4 Address			
05	Type	type	Variable String			
06	Action	action	Variable String			
07	Alert Type	alert	Variable String			
08	Interface Name	i/f_name	Variable String			
09	Interface Dir	i/f_dir	Variable String			
10	Protocol	proto	Variable String			

SECNOLOGY supports all types of event formats including those from your own custom applications without the need for extra toolkits. Using the first and only existing graphical parser on the market, apply rule parsing by simply selecting a field with the mouse.

Create virtual fields to categorize events, add missing information, add time synchronization, turn an original field value into specific information, etc... Do this without affecting the original raw data integrity.

SECNOLOGY The Big Data Mining Company

TURN DATA INTO ACTIONS

Best of Breed Big Data Mining

SECNOLOGY is the only turn-key solution

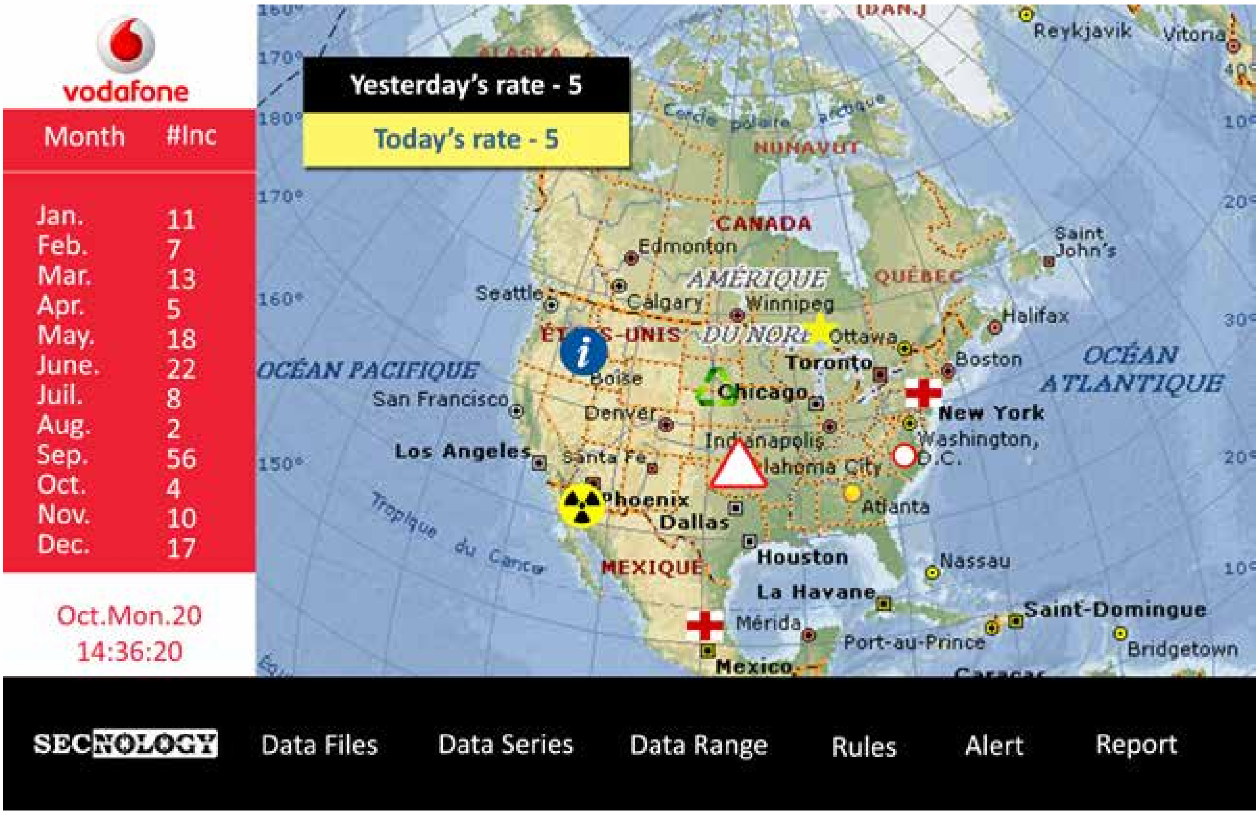
- whose design and architecture does not require a Database
- able to process terabytes a day at no additional cost
- which offers a graphical parser
- that does not need any programming or SDK
- where data and results are always on-line and accessible
- that is ready to use and can be installed in 1 minute
- that does not need dedicated technical resources

Our focus is on making SECNOLOGY very easy to use, very customizable, and very flexible.
SECNOLOGY makes all these operations simple and effective!
SECNOLOGY is the only tool that can analyze and manage your events no matter the origin or type, in real time or on-demand.
SECNOLOGY makes all these operations simple and effective!
SECNOLOGY is able to do everything any other SIEM does, while none of the other SIEM can offer what SECNOLOGY does.

User friendly, customable & flexible

Customers use SECNOLOGY to address many requirements including:

- Event Consolidation
- Regulatory Compliance
- IT & Business Governance
- Alerting, Monitoring & Reporting
- Real-Time Event Management
- Workflow Automation
- Policy Control Management
- Cross Device Event Correlation
- Forensics Event Investigation
- Threat & Risk Management
- Real-Time Monitoring of User Activity
- User Rights and Privileges Auditing
- Data Masking
- File & Folder Change Management
- Configuration Auditing & Analysis
- Data Life Cycle Management
- Application Gateway
- Quality of Service
  Incident Management & Troubleshooting
- Event Response & Real-Time Reaction



vodafone

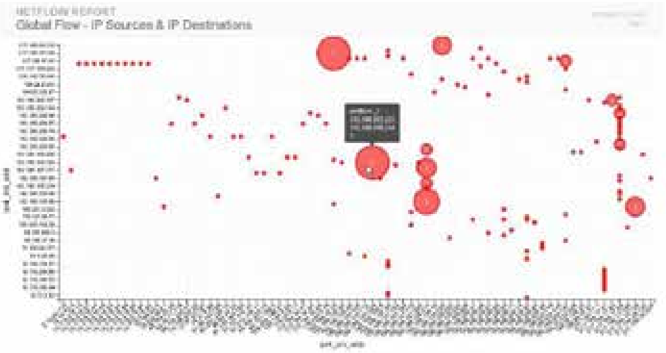
Month	#Inc
Jan.	11
Feb.	7
Mar.	13
Apr.	5
May.	18
June.	22
Juil.	8
Aug.	2
Sep.	56
Oct.	4
Nov.	10
Dec.	17

Oct.Mon.20
14:36:20

Yesterday's rate - 5

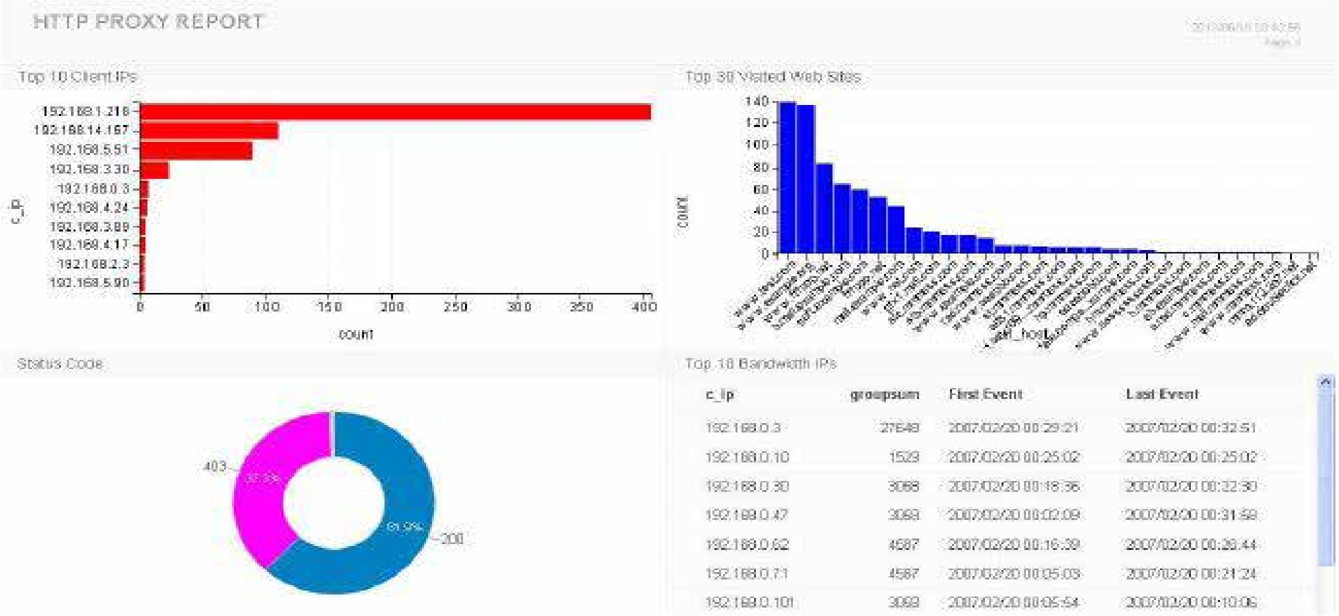
Today's rate - 5

TURN DATA INTO ACTIONS



NETFLOW REPORT

Global Flow - IP Sources & IP Destinations



HTTP PROXY REPORT

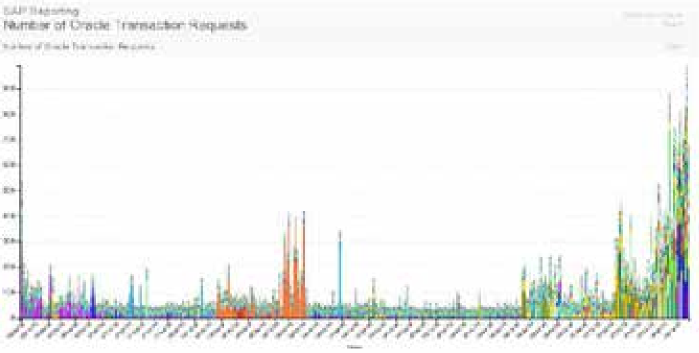
Top 10 Client IPs

Top 30 Visited Web Sites

Status Code

Top 10 Bandwidth IPs

c_ip	groupsum	First Event	Last Event
192.168.0.3	27649	2007/02/20 00:29:21	2007/02/20 00:32:51
192.168.0.10	1529	2007/02/20 00:25:02	2007/02/20 00:25:02
192.168.0.30	3068	2007/02/20 00:18:36	2007/02/20 00:22:30
192.168.0.47	3093	2007/02/20 00:02:09	2007/02/20 00:31:59
192.168.0.62	4587	2007/02/20 00:16:39	2007/02/20 00:28:44
192.168.0.71	4587	2007/02/20 00:05:03	2007/02/20 00:21:24
192.168.0.101	3093	2007/02/20 00:05:54	2007/02/20 00:10:06



SAP Reporting

Number of Oracle Transaction Requests

ANTI VIRUS REPORT

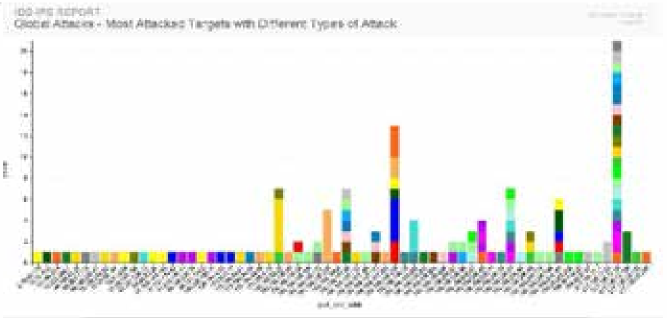
3D - Detected Viruses

HTTP PROXY REPORT

Flow Client IPs - Web Sites

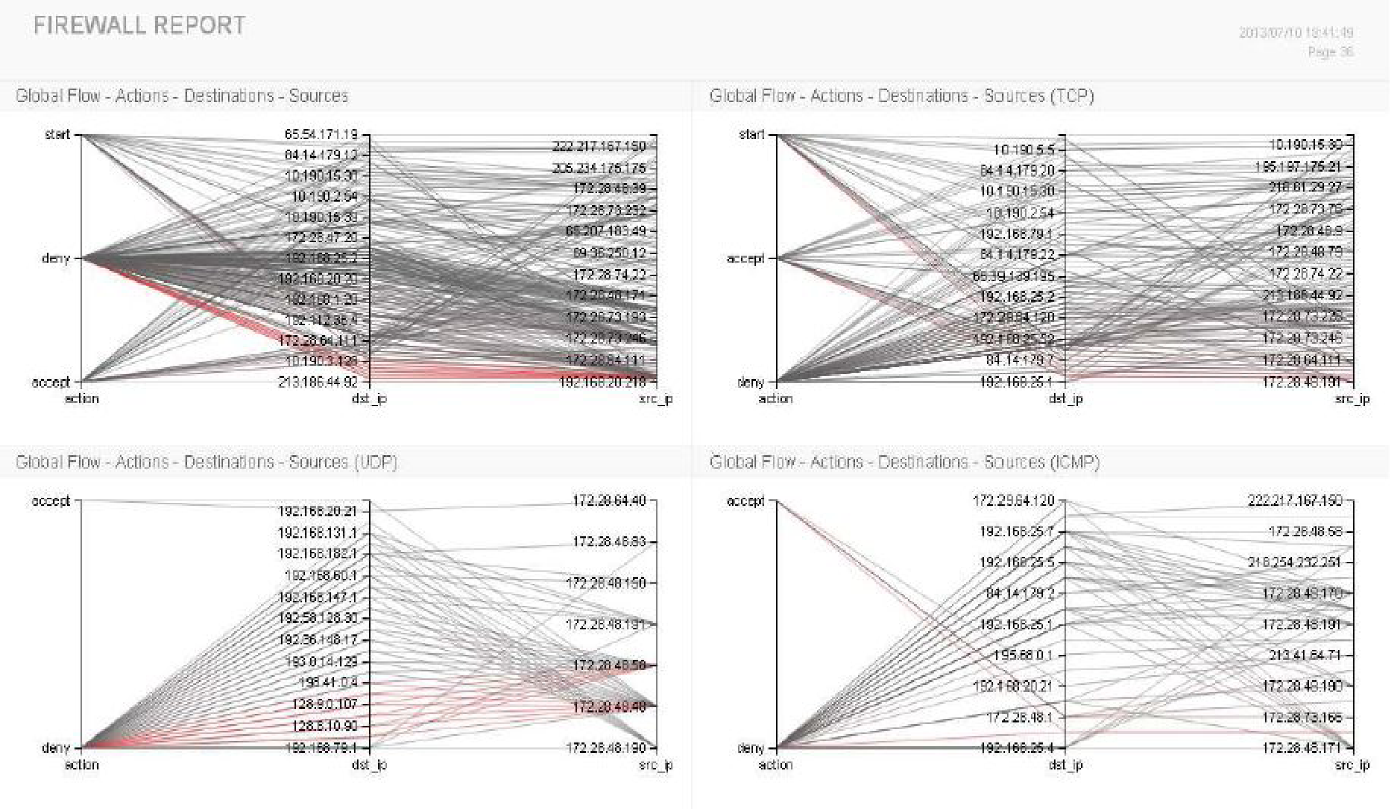
IDS-IPS REPORT

Global Attacks - Most Attacked Targets with Different Types of Attack



IDS-IPS REPORT

Global Attacks - Most Attacked Targets with Different Types of Attack



FIREWALL REPORT

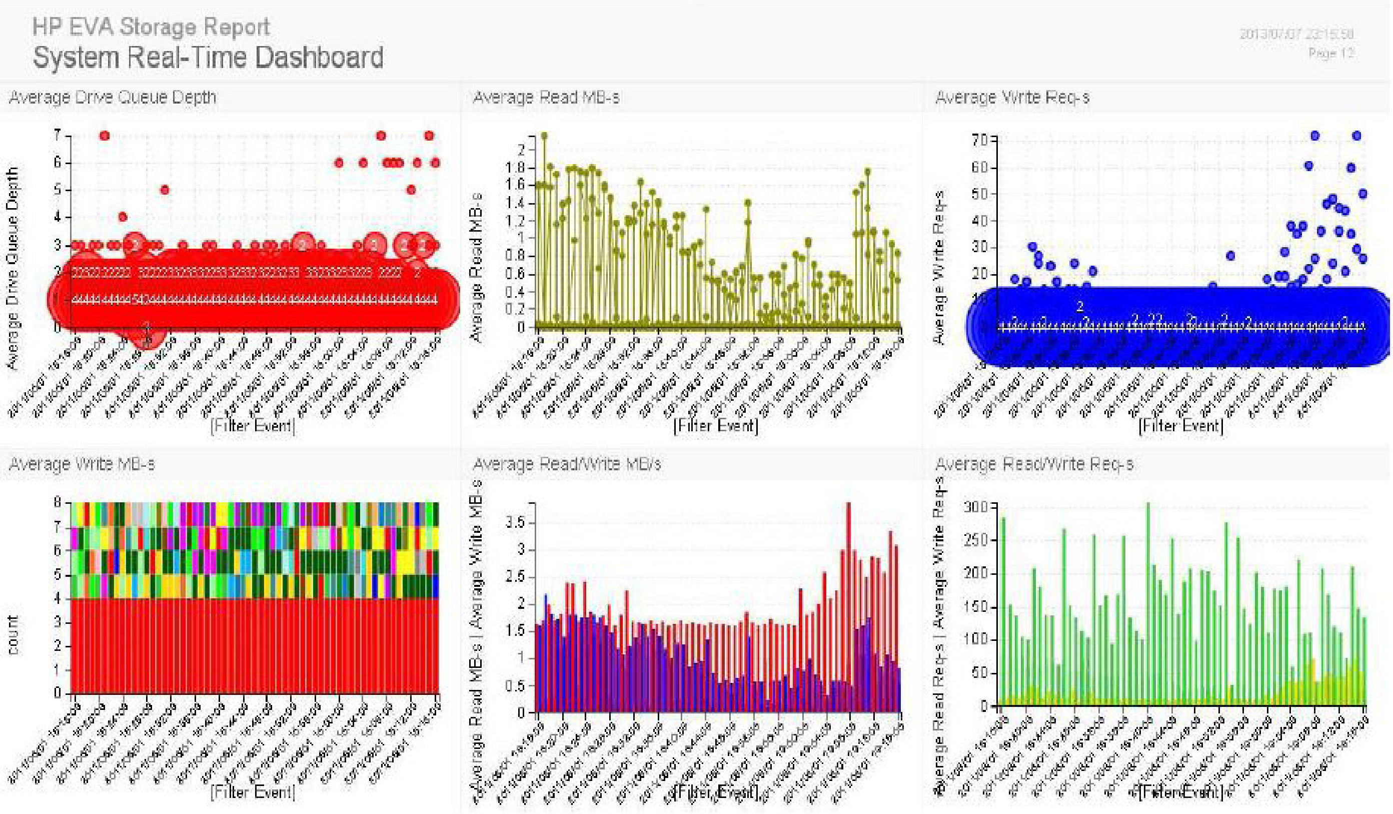
2013/07/10 18:41:49
Page 36

Global Flow - Actions - Destinations - Sources

Global Flow - Actions - Destinations - Sources (TCP)

Global Flow - Actions - Destinations - Sources (UDP)

Global Flow - Actions - Destinations - Sources (ICMP)



HP EVA Storage Report
System Real-Time Dashboard

2013/07/07 23:15:58
Page 12

Average Drive Queue Depth

Average Read MB-s

Average Write Req-s

Average Write MB-s

Average Read/Write MB/s

Average Read/Write Req-s

Average Drive Queue Depth
Average Read MB-s
Average Write Req-s
count
Average Read MB-s | Average Write MB-s
Average Read Req-s | Average Write Req-s
[Filter Event]

Corporate Headquarters
747 El Granada Boulevard Suite 2547
El Granada, CA 94018
(415) 762-1820
info@secnology.com

EMEA Office
22 rue Victor Hugo
78350 Jouy-En-Josas, France
+33 (0)1 4645-4610
emea@secnology.com