



Network Monitoring Tools

CYBER INCIDENT RESPONSE

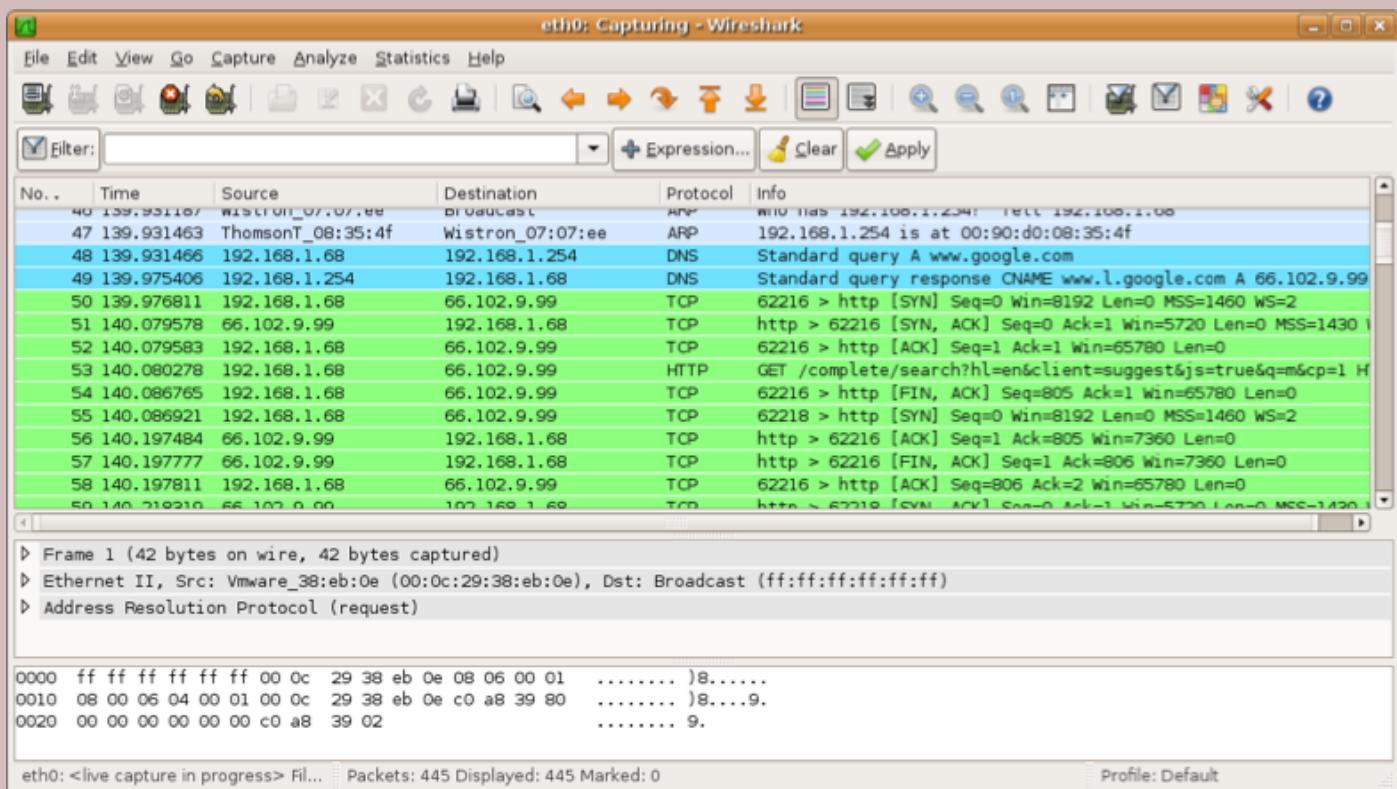
Network Monitoring Tools

- Many network monitoring tools are available for different use cases
- Combination of network data is more powerful than a single piece of data
- Different tools can analyze data in different ways, as well

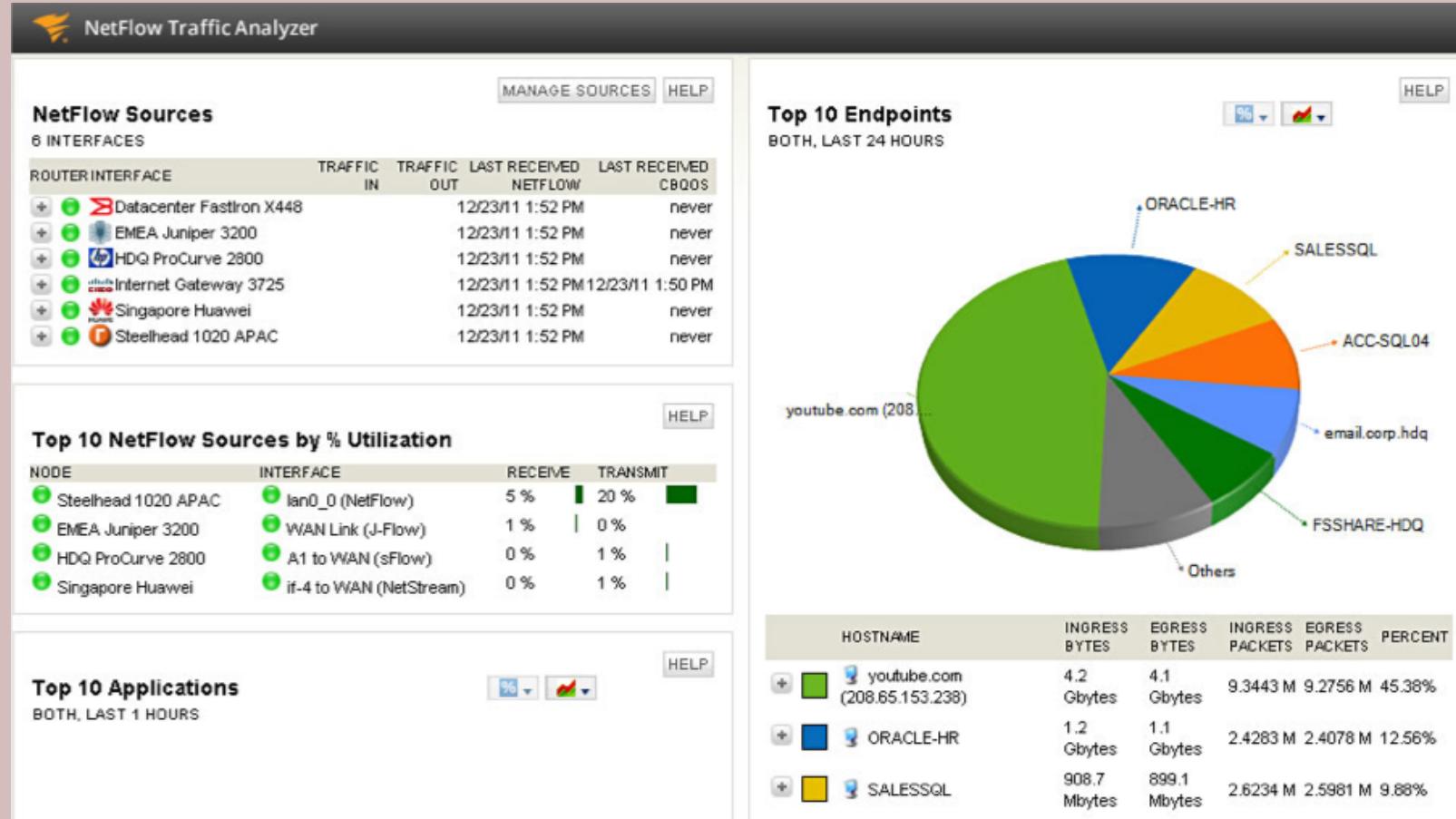


Wireshark

- Passive monitoring and packet capture
- Used for packet analysis



SolarWinds: NetFlow Traffic Analyzer



<http://demo.solarwinds.com>



SolarWinds: Network Performance Monitor

NPM Summary

All Nodes managed by NPM
GROUPED BY REGION

- ▶ ▲ APAC
- ▶ ▲ EMEA
- ▼ ▲ North America
 - 3Com
 - Switch sales
 - American Power Conversion Corp.
 - APC NetBotz
 - Aruba Networks Inc
 - Avaya Communication
 - Cisco
 - Compatible Systems Corp.
 - Dell Computer Corporation
 - Extreme Networks
 - F5 Networks, Inc.
 - FlowPoint Corporation
 - Foundry Networks, Inc.
 - HP
 - IBM
 - Juniper Networks, Inc.
 - Juniper Networks/NetScreen
 - Linksys
 - Linux
 - Meraki Networks, Inc.
 - Multi-Tech Systems, Inc.

Hardware Health Overview

Nodes Count: 37

Status	Count
Up	23
Critical	7
Warning	3
Undefined	4

High Errors & Discards Today
INTERFACES WITH ERRORS+DISCARDS GREATER THAN 10000 TODAY

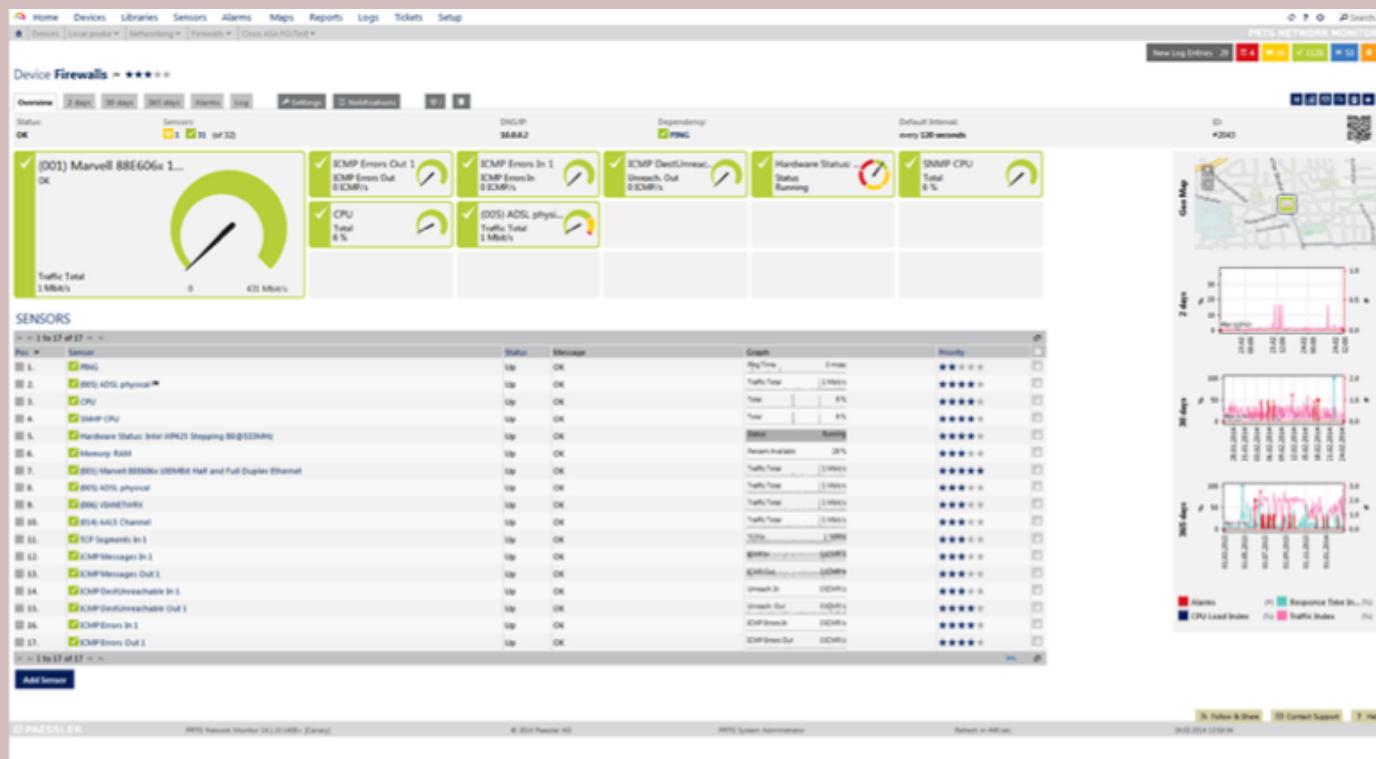
NODE	INTERFACE	RECEIVE ERRORS	RECEIVE DISCARDS	TRANSMIT ERRORS	TRANSMIT DISCARDS
PERM_TEX-MDS9120-76-76	fc1/5	0 errors	0 discards	5,582,170,112 errors	5,808,010 discards
PERM_AP6511-E6C8C0	fe4	64,088,776 errors	78,073,384 discards	0 errors	0 discards
PERM_AP6511-E6C8C0	fe2	100,061,432 errors	2,349 discards	0 errors	0 discards
PERM_TEX-MDS9120-76-76	fc1/6	0 errors	0 discards	5,808,179 errors	10,024,648 discards
PHX-NEXUS 1000V	port-channel1	0 errors	1,244,402 discards	0 errors	0 discards

<http://demo.solarwinds.com>



PRTG

- Paessler Router Traffic Grapher
- Server monitoring, network monitoring, and bandwidth monitoring



- Packet sniffing
 - Monitors packet headers to determine traffic type
- Flows
 - Collects information about connections
- SNMP
 - Network devices report about events through traps
- WMI (Windows Management Instrumentation)
 - Management data of the operating system using scripts or application access



Nagios

- Network and system log monitoring tool
- Provides GUI for system, services, and monitoring capabilities

The screenshot shows the Nagios Fusion web interface with a blue header bar containing 'Home', 'Views', 'Dashboards', 'Configure', 'Help', and 'Admin' links. On the left, there's a sidebar with sections for 'My Dashboards', 'Server Status', 'Alerts', 'Visualizations', and 'Servers'. The 'Servers' section lists several Nagios instances: 'Nagios Uruguay', 'Argentina - IT', 'Nagios Core Demo', 'Nagios Argentina - E.', 'Jujuy', 'Nagios Brasil', 'Nagios Mexico', 'Nagios Colombia', 'Nagios Chile', and 'Nagios Argentina - E. AR'. The main content area displays three status summary cards:

- Nagios Uruguay - Uruguay**

Hosts	0 Up	0 Down	0 Unreachable	0 Pending
Services	0 Ok	0 Warning	0 Unknown	0 Critical 0 Pending

Notifications: Enabled Active Checks: Enabled Passive Checks: Enabled Event Handlers: Enabled

Last Updated: 2013-06-13 11:18:12
- Argentina - IT - Argentina**

Hosts	0 Up	0 Down	0 Unreachable	0 Pending
Services	0 Ok	0 Warning	0 Unknown	0 Critical 0 Pending

Notifications: Enabled Active Checks: Enabled Passive Checks: Enabled Event Handlers: Enabled

Last Updated: 2013-06-13 11:18:12
- Nagios Core Demo - Atlanta, GA**

Hosts	11 Up	0 Down	0 Unreachable	0 Pending
Services	36 Ok	1 Warning 1 Unhandled	0 Unknown	2 Critical 2 Unhandled 0 Pending

Notifications: Enabled Active Checks: Enabled Passive Checks: Enabled Event Handlers: Enabled

Last Updated: 2013-06-13 11:18:12



Nagios

- “Critical” in Nagios isn’t based on CVE’s, but by thresholds you set during config

Nagios

General

- Home
- Documentation

Monitoring

- Tactical Overview
- Service Detail
- Host Detail
- Hostgroup Overview
- Hostgroup Summary
- Hostgroup Grid
- Servicegroup Overview
- Servicegroup Summary
- Servicegroup Grid
- Status Map
- 2-D Status Map
- Service Problems
- Host Problems
- Network Outages

Show Host:

Comments

Downtime

Process Info

Performance Info

Scheduling Queue

Reporting

- Trends
- Availability
- Alert Histogram
- Alert History
- Alert Summary
- Notifications
- Event Log

Configuration

- View Config

Current Network Status

Last Updated: Sun Jan 17 20:52 CET 2006
Updated every 30 seconds
Nagios® - [www.nagios.org](#)
Logged in as z7490r

[View History For All Hosts](#)
[View Notifications For All Hosts](#)
[View Host Status Detail For All Hosts](#)

Host Status Totals

Up	Down	Unreachable	Pending
296	2	0	0

[All Problems](#) [All Types](#)

Service Status Totals

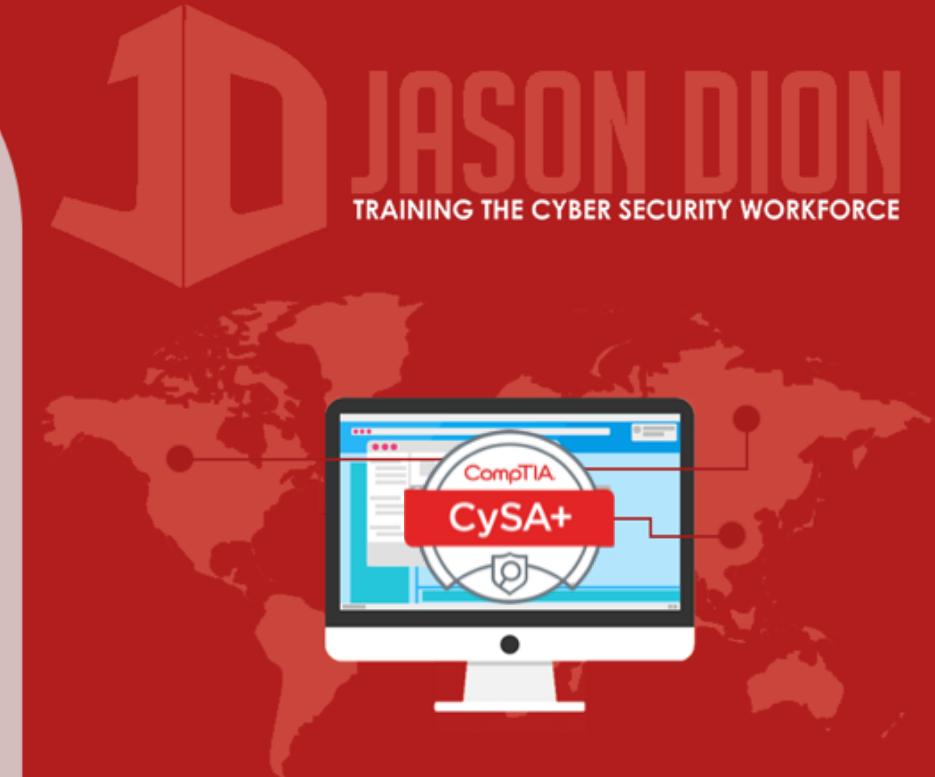
Ok	Warning	Unknown	Critical	Pending
3038	3	2	8	0

[All Problems](#) [All Types](#)

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
LE-LDM001	LinuxShield	CRITICAL	01-01-2006 17:26:12	5d 20h 27m 53s	55	No process matching name found : CRITICAL
LE-LDM002	LinuxShield	CRITICAL	01-01-2006 17:26:26	5d 7h 57m 56s	55	No process matching name found : CRITICAL
EV-MRIS002	N	HP Agent	01-01-2006 17:26:44	2d 7h 53m 6s	15	HP Agents Status Unknown
	NRM	N	01-01-2006 17:27:53	2d 7h 52m 0s	15	CRITICAL - Socket timeout after 10 seconds
	PING	CRITICAL	01-01-2006 17:26:05	2d 7h 51m 48s	15	CRITICAL - Plugin timed out after 10 seconds
EV-JOH002	N	HP Agent	01-01-2006 17:26:05	10d 7h 7m 7s	15	HP Agents Status Unknown
	NRM	N	01-01-2006 17:26:28	10d 7h 6m 10s	15	CRITICAL - Socket timeout after 10 seconds
	PING	CRITICAL	01-01-2006 17:26:45	10d 7h 7m 6s	15	CRITICAL - Plugin timed out after 10 seconds
EV-GMUND02	N	HP Agent	01-01-2006 17:28:15	0d 2h 11m 58s	55	HP Agents Status Degraded
EV_HALL02	N	HP Agent	01-01-2006 17:25:04	0d 23h 28m 0s	55	HP Agents Status Degraded
EV_MANI02	N	HP Agent	01-01-2006 17:27:54	2d 11h 41m 10s	55	HP Agents Status Failed
EV_SPIT02	N	HP Agent	01-01-2006 17:28:31	6d 21h 1m 37s	55	HP Agents Status Degraded
EV_TAM002	N	HP Agent	01-01-2006 17:27:23	13d 4h 32m 10s	55	HP Agents Status Failed

13 Matching Service Entries Displayed



Cacti

- Uses SNMP polling of network devices for status information and shows a GUI

