



Network Monitoring Tools

CYBER INCIDENT RESPONSE

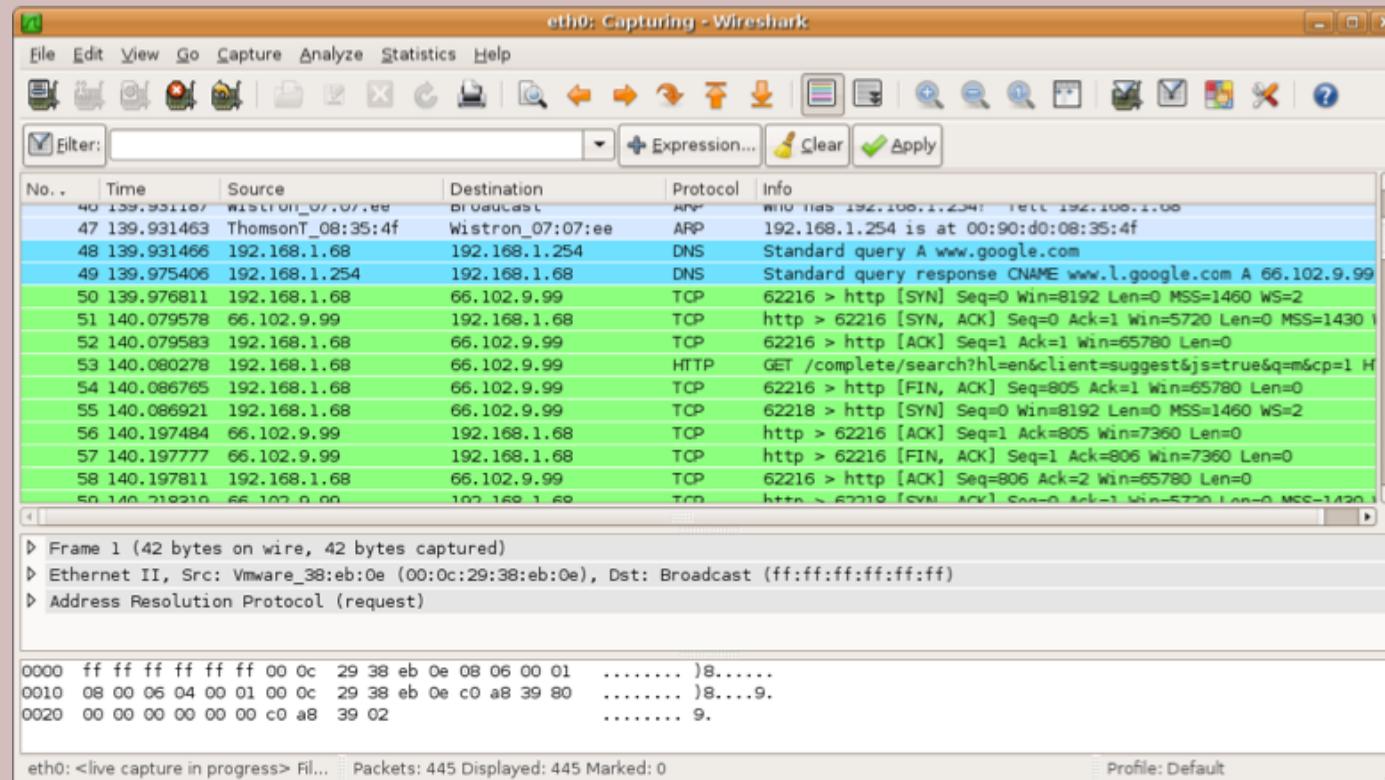
Network Monitoring Tools

- 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



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

NetFlow Traffic Analyzer

NetFlow Sources
6 INTERFACES

ROUTER INTERFACE	TRAFFIC IN	TRAFFIC OUT	LAST RECEIVED NETFLOW	LAST RECEIVED CBQOS
Datacenter Fastron X448			12/23/11 1:52 PM	never
EMEA Juniper 3200			12/23/11 1:52 PM	never
HDQ ProCurve 2800			12/23/11 1:52 PM	never
Internet Gateway 3725			12/23/11 1:52 PM	12/23/11 1:50 PM
Singapore Huawei			12/23/11 1:52 PM	never
Steelhead 1020 APAC			12/23/11 1:52 PM	never

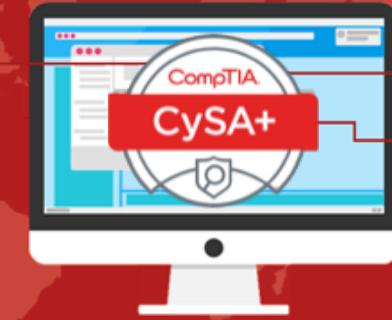
Top 10 NetFlow Sources by % Utilization

NODE	INTERFACE	RECEIVE	TRANSMIT
Steelhead 1020 APAC	lan0_0 (NetFlow)	5 %	20 %
EMEA Juniper 3200	WAN Link (J-Flow)	1 %	0 %
HDQ ProCurve 2800	A1 to WAN (sFlow)	0 %	1 %
Singapore Huawei	if-4 to WAN (NetStream)	0 %	1 %

Top 10 Endpoints
BOTH, LAST 24 HOURS

HOSTNAME	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
youtube.com (208.65.153.238)	4.2 Gbytes	4.1 Gbytes	9.3443 M	9.2756 M	45.38%
ORACLE-HR	1.2 Gbytes	1.1 Gbytes	2.4283 M	2.4078 M	12.56%
SALESSQL	908.7 Mbytes	899.1 Mbytes	2.6234 M	2.5981 M	9.88%

Top 10 Applications
BOTH, LAST 1 HOURS



<http://demo.solarwinds.com>

SolarWinds: Network Performance Monitor

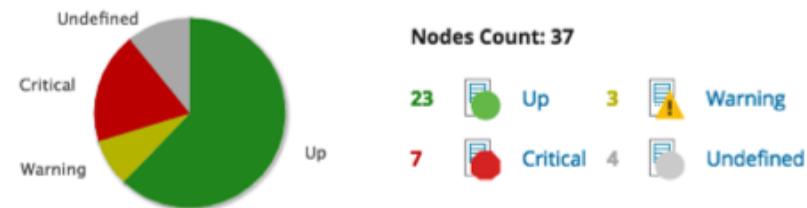


NPM Summary

All Nodes managed by NPM GROUPED BY REGION

- ▶ ▲ APAC
- ▶ ▲ EMEA
- ▼ ▲ North America
 - 3Com
 - Switch sales
 - American Power Conversion Co.,p.
 - 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



High Errors & Discards Today

INTERFACES WITH ERRORS+DISCARDS GREATER THAN 10000 TODAY

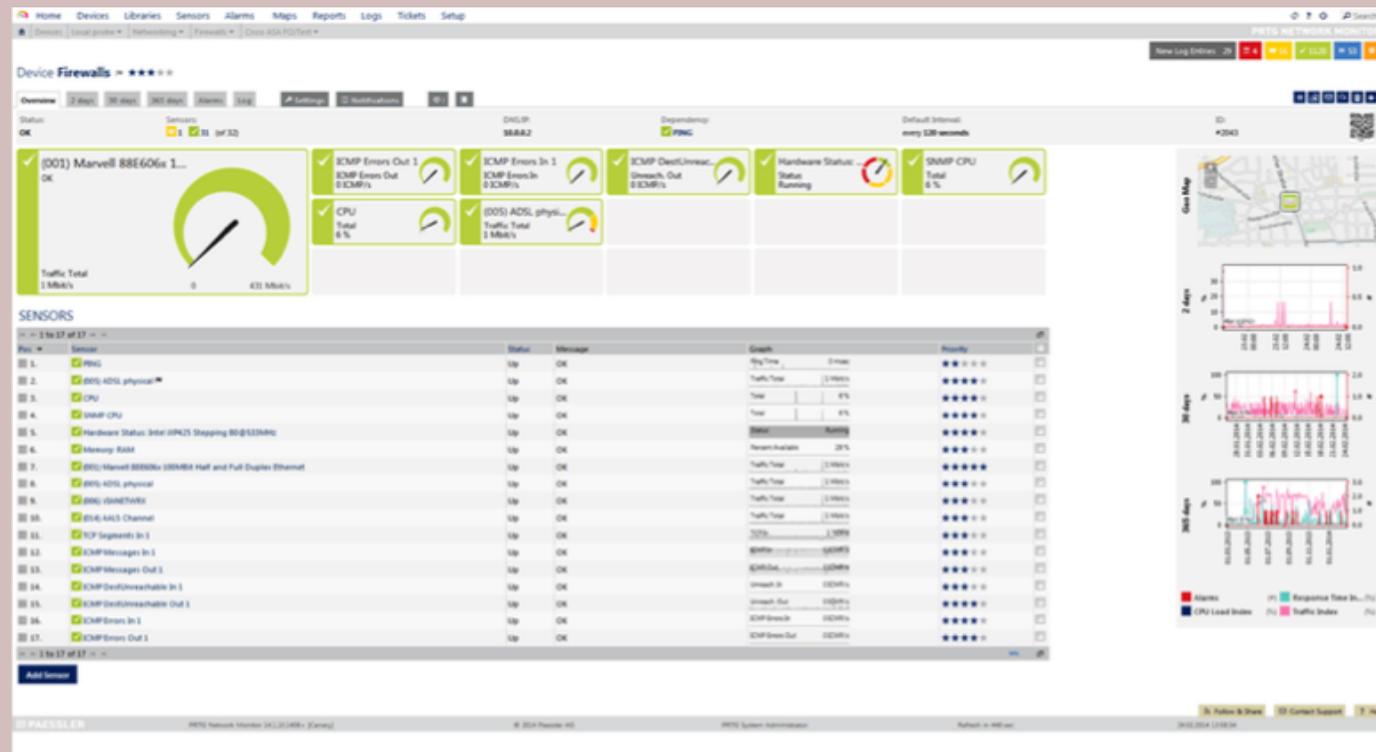
NODE	INTERFACE	RECEIVE ERRORS	RECEIVE DISCARDS	TRANSMIT ERRORS	TRANSMIT DISCARDS
PERM_TEX-MDS9120-76-76	fc1/5	0 errors	0 discards	5,582,170,112 errors	5,808,010 discards
PERM_AP6511-E6C8C0	fe4	64,088,776 errors	78,073,384 discards	0 errors	0 discards
PERM_AP6511-E6C8C0	fe2	100,061,432 errors	2,349 discards	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



PRTG

- 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 displays the Nagios Fusion web interface. The top navigation bar includes 'Home', 'Views', 'Dashboards', 'Configure', 'Help', and 'Admin'. A left sidebar lists 'My Dashboards' (Home Page, Server Status, Alerts, Visualizations, Servers) and a tree view of servers including Nagios Uruguay, Argentina - IT, Nagios Core Demo, and others. The main content area shows three monitoring dashboards:

- Nagios Uruguay - Uruguay**: Status Summary shows 0 Up, 0 Down, 0 Unreachable, 0 Pending, 0 Ok, 0 Warning, 0 Unknown, 0 Critical, 0 Pending. Settings: Notifications: Enabled, Active Checks: Enabled, Passive Checks: Enabled, Event Handlers: Enabled. Last Updated: 2013-06-13 11:18:12.
- Argentina - IT - Argentina**: Status Summary shows 0 Up, 0 Down, 0 Unreachable, 0 Pending, 0 Ok, 0 Warning, 0 Unknown, 0 Critical, 0 Pending. Settings: Notifications: Enabled, Active Checks: Enabled, Passive Checks: Enabled, Event Handlers: Enabled. Last Updated: 2013-06-13 11:18:12.
- Nagios Core Demo - Atlanta, GA**: Status Summary shows 11 Up, 0 Down, 0 Unreachable, 0 Pending, 36 Ok, 1 Warning, 0 Unknown, 2 Critical, 1 Unhandled, 2 Unhandled, 0 Pending. Settings: 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

The screenshot displays the Nagios web interface. On the left is a navigation sidebar with sections for General, Monitoring, Reporting, and Configuration. The main content area shows 'Current Network Status' (Last Updated: Sun Jan 1 17:28:52 CET 2006), 'Host Status Totals' (Up: 2, Down: 0, Unreachable: 0, Pending: 0), and 'Service Status Totals' (Ok: 13, Warning: 3, Unknown: 2, Critical: 8, Pending: 0). Below these are 'Display Filters' and a table titled 'Service Status Details For All Hosts'.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
US-DMZ001	LinuxShield	CRITICAL	01-01-2006 17:25:12	5d 20h 27m 53s	5/5	No process matching name found - CRITICAL
US-DMZ002	LinuxShield	CRITICAL	01-01-2006 17:26:26	5d 7h 57m 56s	5/5	No process matching name found - CRITICAL
SV-QH202	HPAgent	UNKNOWN	01-01-2006 17:26:44	2d 7h 53m 6s	1/5	HP Agent Status Unknown
	NBM	CRITICAL	01-01-2006 17:27:53	2d 7h 52m 0s	1/5	CRITICAL - Socket timeout after 10 seconds
	PING	CRITICAL	01-01-2006 17:25:05	2d 7h 51m 48s	1/5	CRITICAL - Plugin timed out after 10 seconds
SV-QH202	HPAgent	UNKNOWN	01-01-2006 17:25:05	10d 7h 7m 7s	1/5	HP Agent Status Unknown
	NBM	CRITICAL	01-01-2006 17:25:28	10d 7h 5m 18s	1/5	CRITICAL - Socket timeout after 10 seconds
	PING	CRITICAL	01-01-2006 17:26:45	10d 7h 7m 8s	1/5	CRITICAL - Plugin timed out after 10 seconds
SV-OML002	HPAgent	WARNING	01-01-2006 17:28:15	0d 2h 11m 58s	5/5	HP Agent Status Degraded
SV-HALL02	HPAgent	WARNING	01-01-2006 17:25:04	0d 23h 38m 0s	5/5	HP Agent Status Degraded
SV-MAN02	HPAgent	CRITICAL	01-01-2006 17:27:14	3d 11h 41m 10s	5/5	HP Agent Status Failed
SV-SP102	HPAgent	WARNING	01-01-2006 17:29:21	5d 21h 1m 37s	5/5	HP Agent Status Degraded
SV-TAM02	HPAgent	CRITICAL	01-01-2006 17:27:23	13d 4h 32m 10s	5/5	HP Agent Status Failed

13 Matching Service Entries Displayed



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE



Catci

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

