JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Network Monitoring Tools

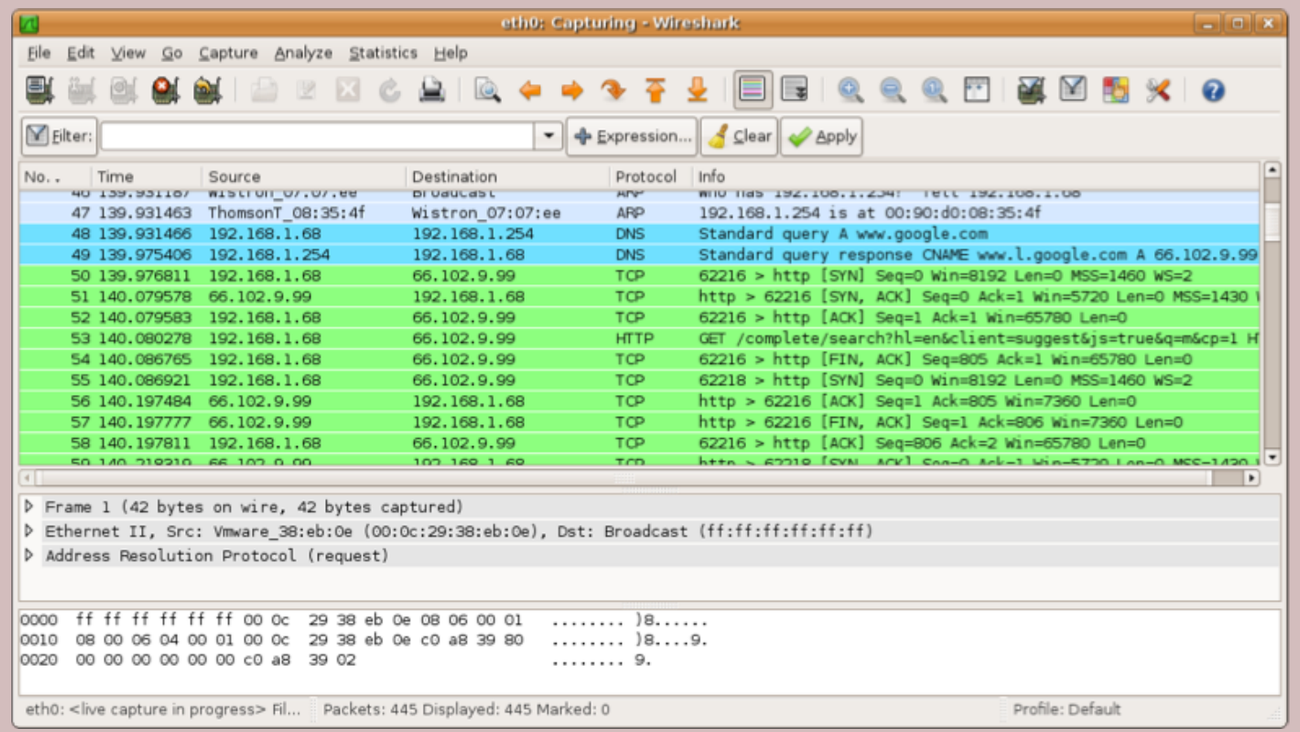
CYBER INCIDENT RESPONSE

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

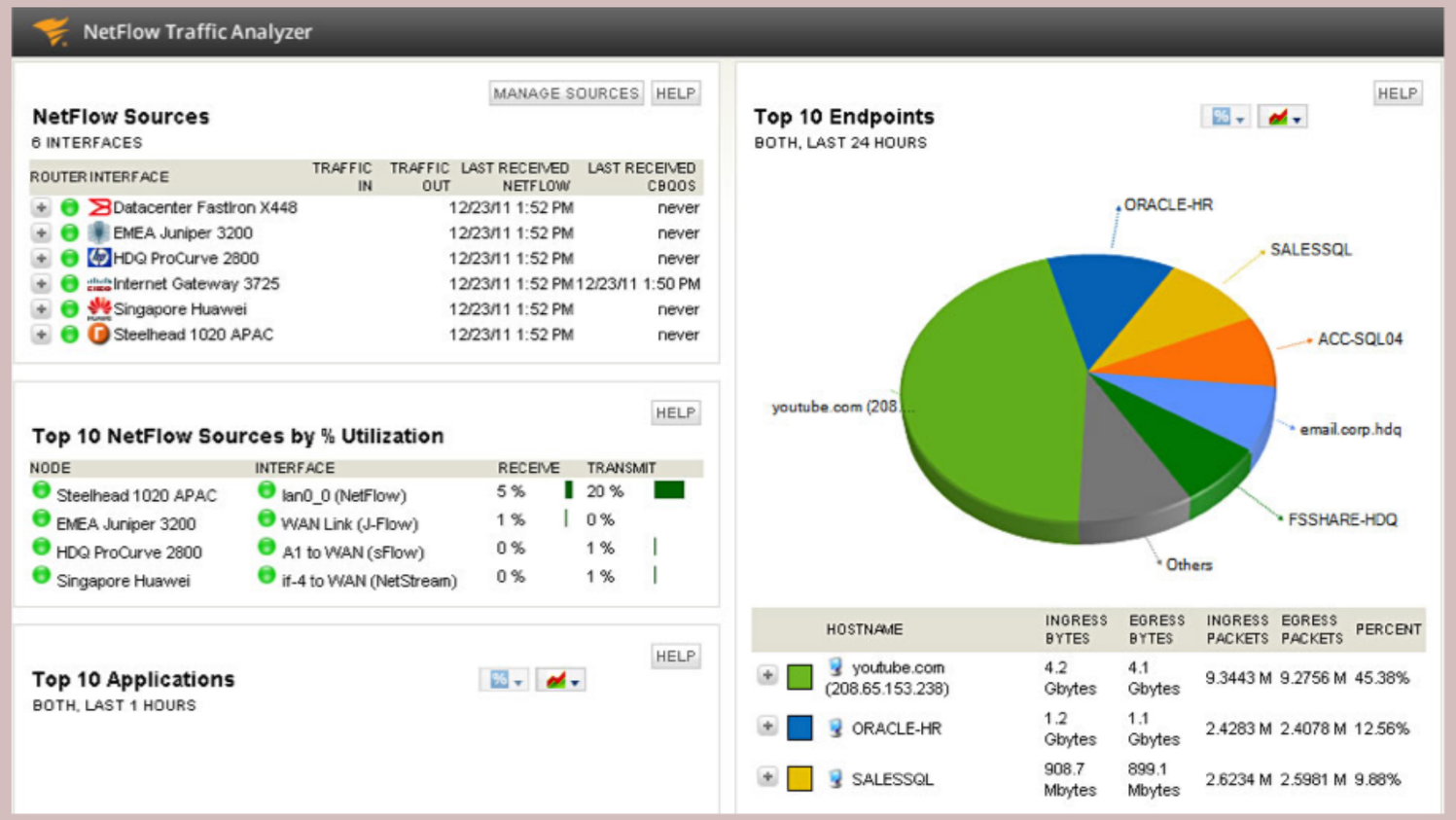
Wireshark

- Passive monitoring and packet capture
- Used for packet analysis



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

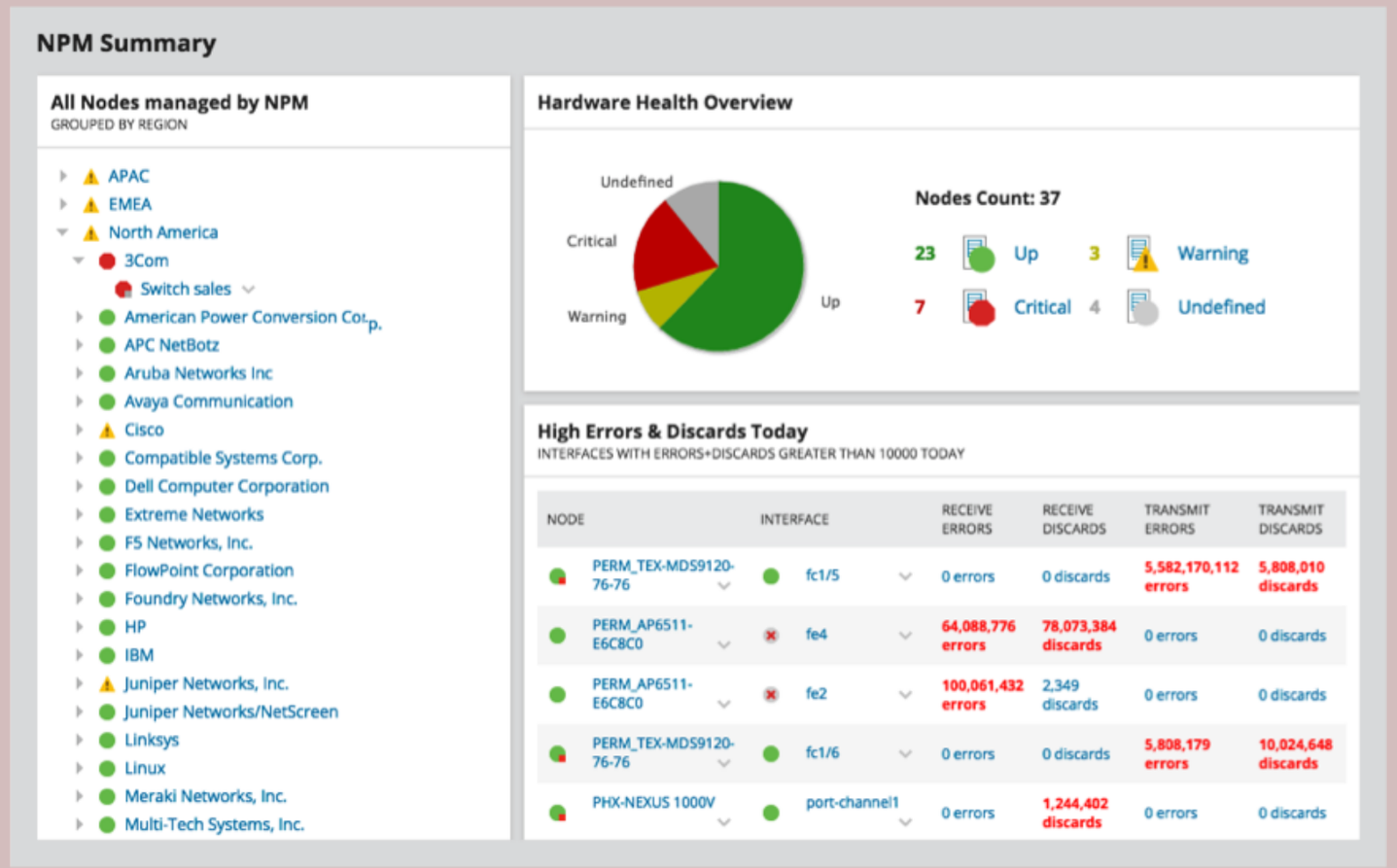
SolarWinds: Netflow Traffic Analyzer



http://demo.solarwinds.com

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

SolarWinds:
Network Performance Monitor

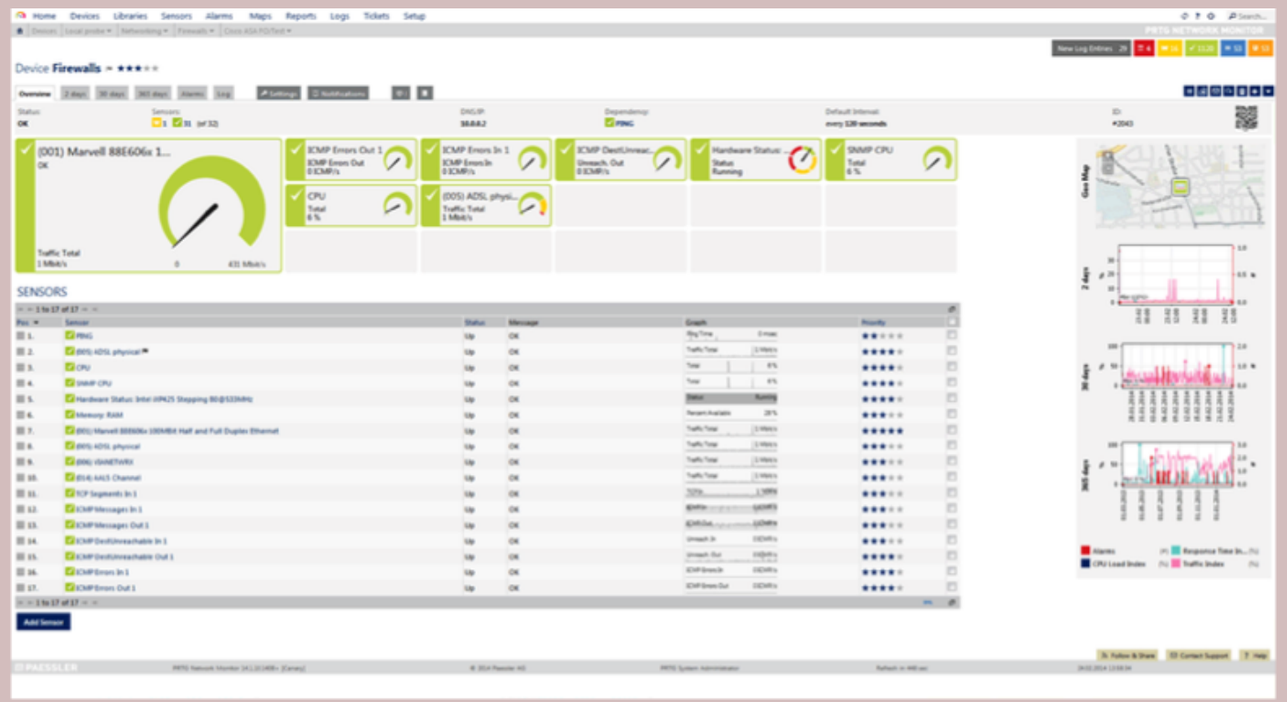


http://demo.solarwinds.com

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

PRTG

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



PRTG

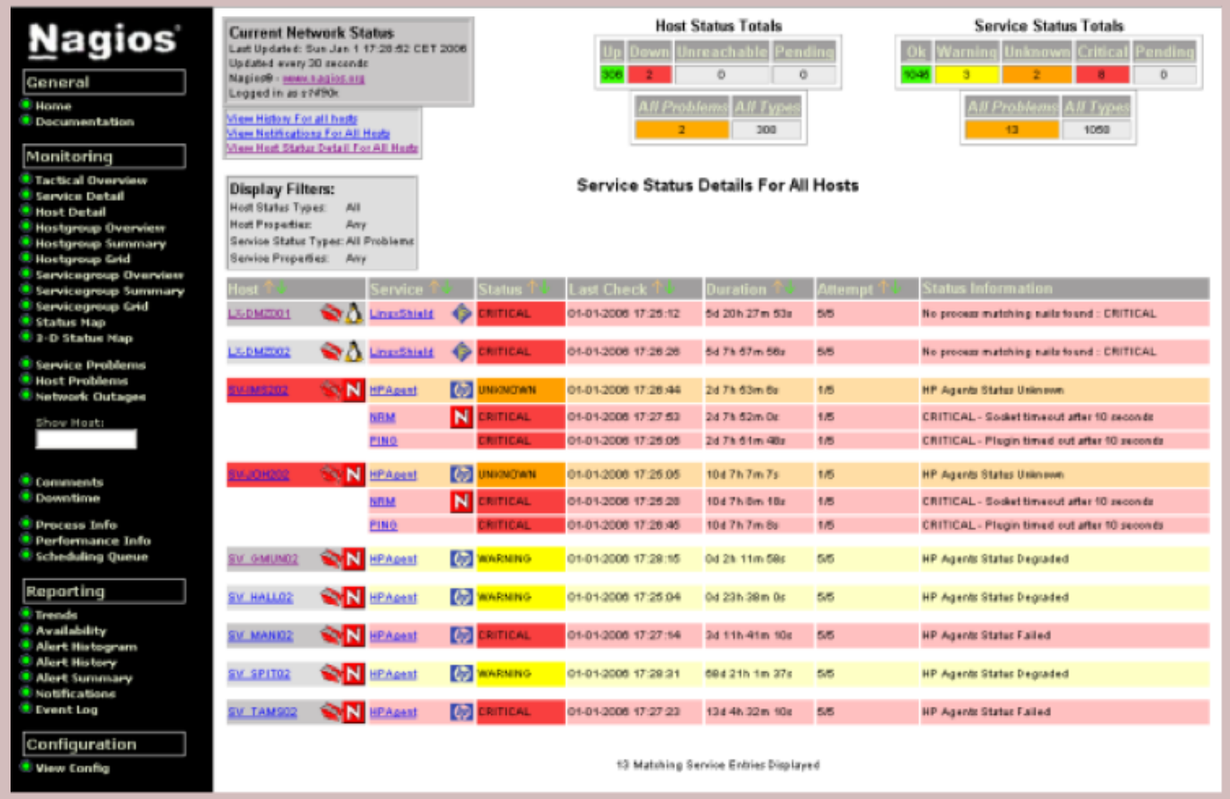
- Packet sniffing
  - Monitors packet headers to determine traffic type
- Flows
  - Collects information about connections
- SNMP
  - Network devices report about events through traps
- WMI (Windows Management Instrumentation)
  - Management data of the operating system using scripts or application access

Nagios

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

Nagios

- "Critical" in Nagios isn't based on CVE's, but by thresholds you set during config



Catci

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