RAVEN, Network Security and Health for the Enterprise

The Promia RAVEN is a hardened Security Information and Event Management (SIEM) solution further providing network health, and interactive visualizations for enterprise network mapping and leak detection (ENMLDS).

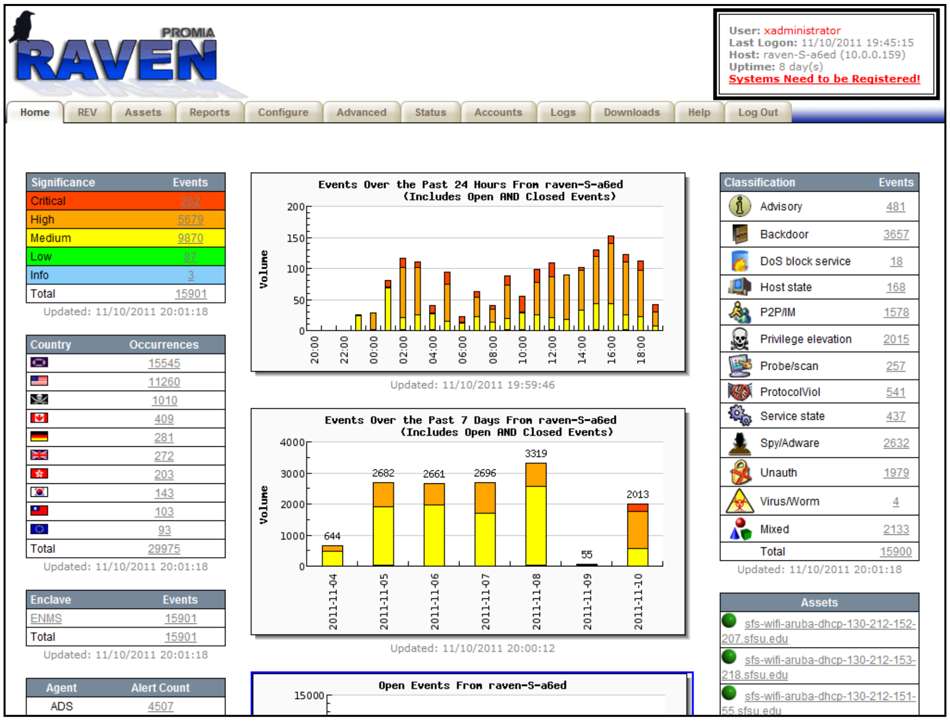
RAVEN safeguards your network because it supports the full network security lifecycle:

- **Discovers** - RAVEN's enterprise network mapping (ENM) capability finds a network's entry and exit points as well as all the assets (computers, routers, modems, switches, etc.) on the network so it knows what to protect. It also monitors asset state.

- **Detects/Protects** - RAVEN enforces policies, watches network activity and protects your network. It performs signature matching, anomaly detection, blocking and other analysis in real-time. Bandwidth analysis and reporting was developed in collaboration with, and is deployed by, the U.S. Navy. Unlike standalone SIEM products, RAVEN further incorporates vital security operation functions including network and component health monitoring as part of keeping your enterprise network functioning.

- **Reacts/Alerts** - RAVEN will react to an attack. It can alert the proper people that something is happening that needs attention which includes bandwidth anomalies. It can also be set up to take action such as blocking traffic to or from a known malware site.

- **Presents** - RAVEN displays the security issues that are happening on your network in a web browser based display. A dashboard reports on levels of attack (incident, alerts) with options to drill into incident details and even the triggering network packet itself, where these events are sliced and diced into different categories and graphs, as shown below.



User: xadministrator
Last Logon: 11/10/2011 19:45:15
Host: raven-S-a6ed (10.0.0.159)
Uptime: 8 day(s)
Systems Need to be Registered!

Significance	Events
Critical	262
High	5679
Medium	9870
Low	87
Info	3
Total	15901

Updated: 11/10/2011 20:01:18

Country	Occurrences
	15545
🇺🇸	11260
🏴‍☠️	1010
🇨🇦	409
🇩🇪	281
🇬🇧	272
🇭🇰	203
🇰🇷	143
🇹🇼	103
🇪🇺	93
Total	29975

Updated: 11/10/2011 20:01:18

Enclave	Events
ENMS	15901
Total	15901

Updated: 11/10/2011 20:01:18

Agent	Alert Count
ADS	4507

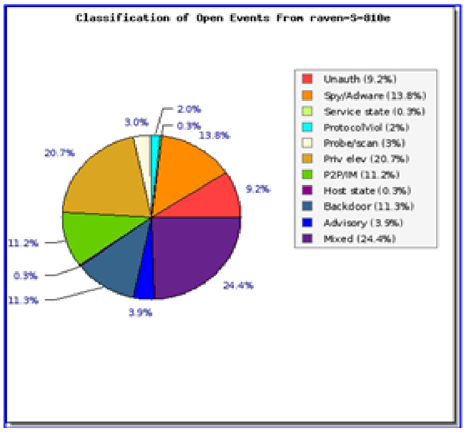
Updated: 11/10/2011 19:59:46

Updated: 11/10/2011 20:00:12

Classification	Events
Advisory	481
Backdoor	3657
DoS block service	18
Host state	168
P2P/IM	1578
Privilege elevation	2015
Probe/scan	257
ProtocolViol	541
Service state	437
Spy/Adware	2632
Unauth	1979
Virus/Worm	4
Mixed	2133
Total	15900

Updated: 11/10/2011 20:01:18

Assets
● sfs-wifi-aruba-dhcp-130-212-152-207.sfsu.edu
● sfs-wifi-aruba-dhcp-130-212-153-218.sfsu.edu
● sfs-wifi-aruba-dhcp-130-212-151-55.sfsu.edu



How RAVEN Helps Your Enterprise Security Operations

RAVEN keeps all levels of your enterprise informed:

- RAVEN’s hierarchical architecture gets the right information to the right people. It propagates information up from branches to regional offices to corporate offices allowing upper management as well as local management to have a clear view of the corporate network’s health.

RAVEN makes it easy to implement a consistent incident detection and response policy:

- Security policy changes and software updates can be pushed down from the corporate offices to regional offices and then to branches. RAVEN unifies security policy management across all deployed instances.

RAVEN's browser user interface consolidates network security, health and mapping:

- The web-based RAVEN user interface includes capabilities for defining site-specific policy-driven responses, incident review, and incident closure. Incident review includes the ability to drill into the actual network packets responsible for the alert for forensic analysis.

- Fundamental to efficient network operations and incident review is the knowledge of what systems and services are on the network. That information is discovered by the RAVEN enterprise network mapping (ENM) capability and is presented in both 2D and 3D formats.

RAVEN is scalable across your enterprise:

- RAVEN is capable of monitoring and managing the regional or departmental security operations of a large enterprise. Multiple RAVENs can watch individual portions of an enterprise’s network and aggregate alerts up and through the enterprise’s top level so you are aware of widespread issues. Likewise, incident detection and response security policies may be efficiently pushed downward.

- Whether a single RAVEN is installed or a hundred, they can all see each other’s events and their discovered network assets allowing for detection of a distributed attack. While it can be deployed alone for network protection of a small to medium-sized network, RAVEN is most effective when used to consolidate events coming in from a group of networks. One security team can efficiently manage operations across many distributed sites.

RAVEN Increases Security Team Efficiency

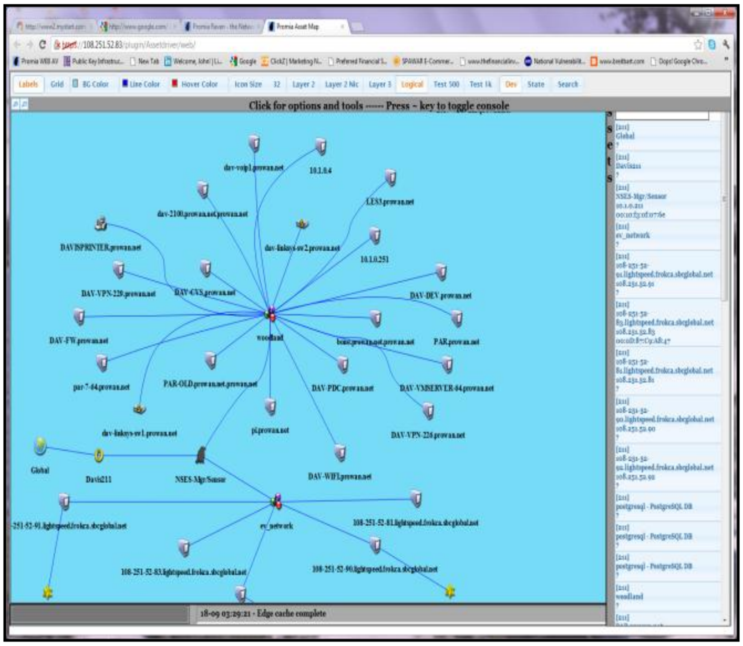
A network security threat will frequently be discovered repeatedly over time such as a ping across a set of computers. Rather than sending an alert for each of the threats (i.e. one for each computer probed), RAVEN aggregates similar alerts into a one incident which can be more efficiently managed. RAVEN supports customized signatures to additionally discover threats unique to your enterprise. RAVEN also monitors your network for unusual behavior. The result is the ability to identify more threats while sending fewer false alarms. Furthermore, RAVEN's hierarchical deployment feature propagates summary information upward to share this knowledge for broader network operations intelligence. Bandwidth trend analysis, monitoring and automated alerts help network personnel efficiently perform their duties. In addition, real-time indexing of IP interactions provides robust forensic search capabilities.

Enterprise Network Mapping & Leak Detection System (ENMLDS)

The Enterprise Network Mapping and Leak Detection System (ENMLDS) was mandated by the U.S. government to locate unauthorized networks, machines, and connection points, and prevent leaks of sensitive data to unknown network intruders. RAVEN's ENMLDS solution consists of a secure network appliance that is active across a multi-layered network architecture. It can be managed using a web browser and can discover, map, and detect the presence or absence of unauthorized network connections. The ENMLDS solution can perform these tasks across an entire network, as well as, specific network segments or local enclaves.

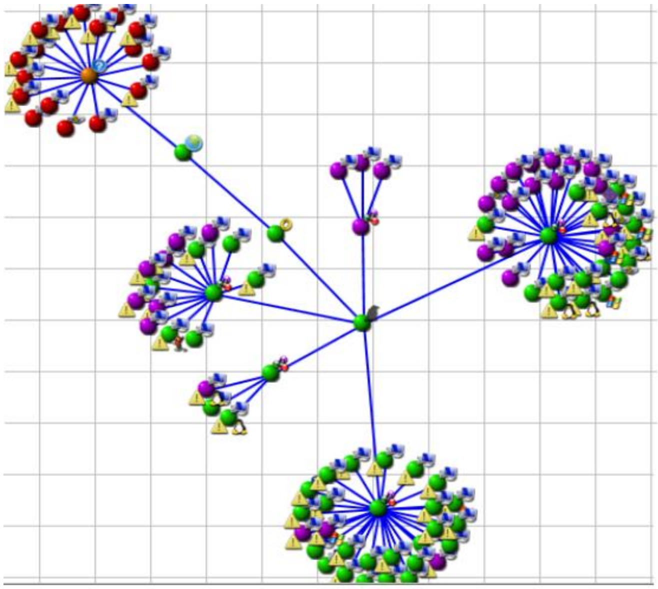
Enterprise Network Mapping (ENM)

Enterprise Network Maps are visual representations of various aspects of your networks, depending on the size and number of networks within the enterprise. This knowledge is mainly gathered passively by listening to network traffic. Using techniques such as packet header inspection and device fingerprinting the Layer 2 and layer 3 topologies are determined and presented visually to the users. RAVEN uses active probing to gather information such as Simple Network Management Protocol (SNMP) details of various devices such as routers and switches. A "rogue" host or network is any host or network that appears on a monitored network that it should not be on. For example, if somebody sets up a new LAN on an existing network, that LAN network is rogue as it is not in the list of authorized networks. Likewise a never before seen host is rogue as well.



Leak Detection\Defense System (LDS)

RAVEN's ENMLDS feature enables leak detection by taking a snapshot of a network at several levels of the OSI model, specifically Level 2 (Data Link Layer) and Layer 3 (Network Layer), on a regular basis. Any differences from the known topology of the network may be considered unauthorized and a possible threat. Any new connections or hosts on the network can be interrogated to see if they have authorization to be on the network. If not, action can be taken to remove the host(s) or unauthorized network from accessing the network. Leak detection also includes ex-filtration and rogue host detection. Ex-filtration is the leaking of data across network boundaries. ENMLDS is able to stop ex-filtration via a proxy list and a watch list. This can be as simple as making something available that should not be, or as complex as a hacker siphoning off data. A proxy list is a list of known proxies that ENMLDS can alert upon observing and block. A watch list is a list of hosts from which ENMLDS can trigger alerts and block.



RAVEN IDS and IPS Capabilities

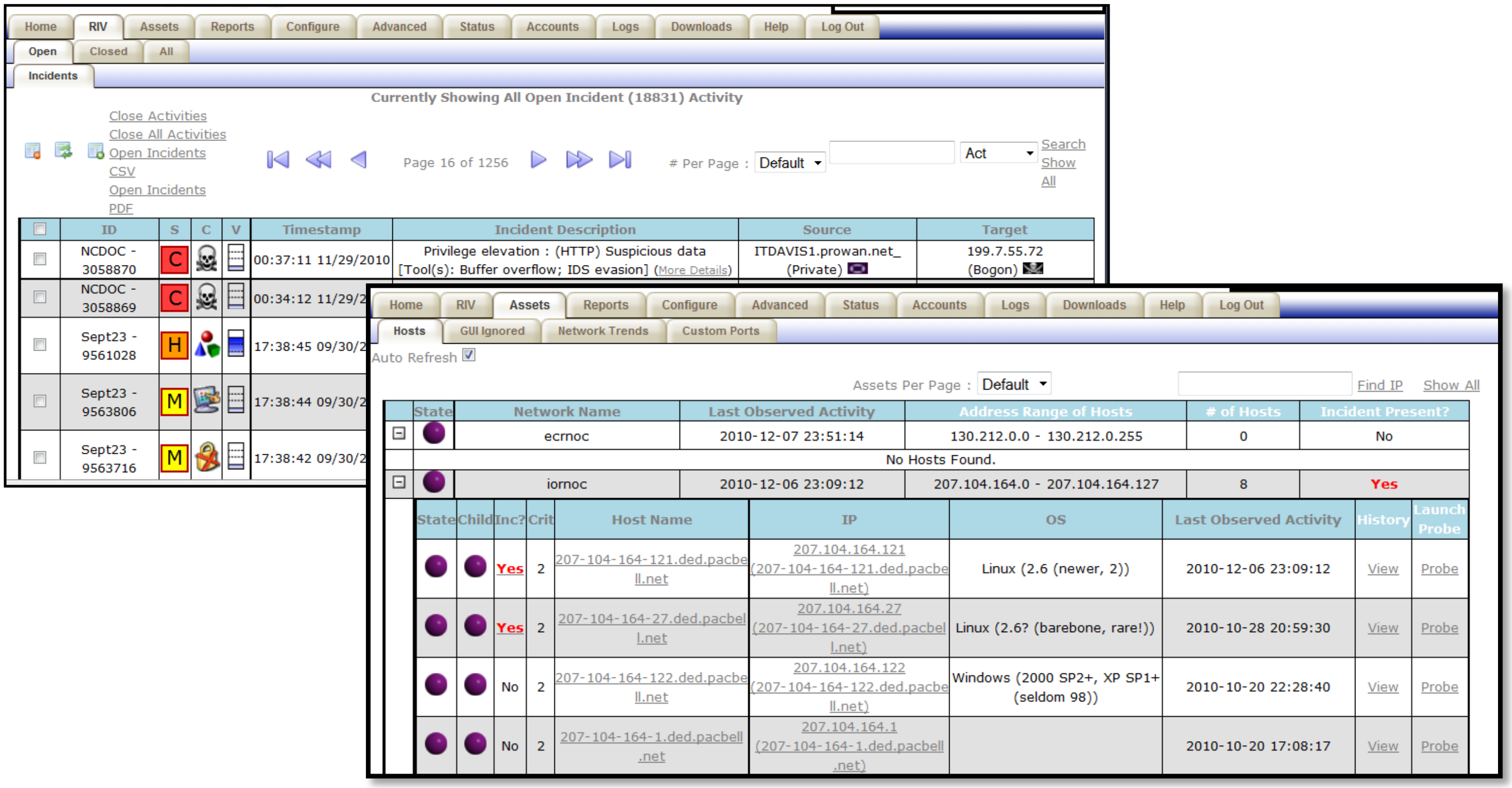
Network Sensor and Analytics

RAVEN's analytics detects operational and security incidents that would not otherwise be visible from any single sensor. The software uses a unique combination of expert system and statistical aggregation and correlation algorithms to analyze events from multiple sensor sources. An additional result of the algorithms is a natural language description of the kind of incident detected. RAVEN has a performance enhanced implementation of Snort as its core internal sensor. RAVEN external sensor data may be in syslog, Windows event record, Host Based Security System (HBSS), or ArcSight Common Event Expression (CEE) format. These alerts may be correlated and aggregated as with the internal sensor generated alerts.

The RAVEN Network Security Event Sensor (NSES) has several network traffic analyzers. One analyzer passively identifies, fingerprints, and maps network assets. Traffic from unknown hosts is reported as suspicious. Another analyzer uses the Snort engine to compare network packets with IDS attack signature patterns that have been developed by the Snort community and independently tested by Promia. The sensor includes filters that use local knowledge to eliminate false positive events, aggregate consecutive instances of the same event, and filter\report events according to proxy, white and black lists of IP addresses.

Customizable and Reactive Rules

NSES also has Policy Management (IP/port/protocol), URL/DNS, and IPS blocking. IPS blocking is where Snort signatures are matched against created alerts, to automatically add that alert's "non-monitored host" (a foreign host not within the monitored network) IP to either the Watch list or Proxy list. This is a real-time function, where IPs are immediately added to the applicable lists as alerts are created. Then, all similar future traffic will be either blocked or reported, based on the operator selected list options.



Currently Showing All Open Incident (18831) Activity

☐	ID	S	C	V	Timestamp	Incident Description	Source	Target
☐	NCDOC - 3058870	C	☠		00:37:11 11/29/2010	Privilege elevation : (HTTP) Suspicious data [Tool(s): Buffer overflow; IDS evasion] (More Details)	ITDAVIS1.prowan.net_ (Private)	199.7.55.72 (Bogon)
☐	NCDOC - 3058869	C	☠		00:34:12 11/29/2			
☐	Sept23 - 9561028	H			17:38:45 09/30/2			
☐	Sept23 - 9563806	M			17:38:44 09/30/2			
☐	Sept23 - 9563716	M			17:38:42 09/30/2			

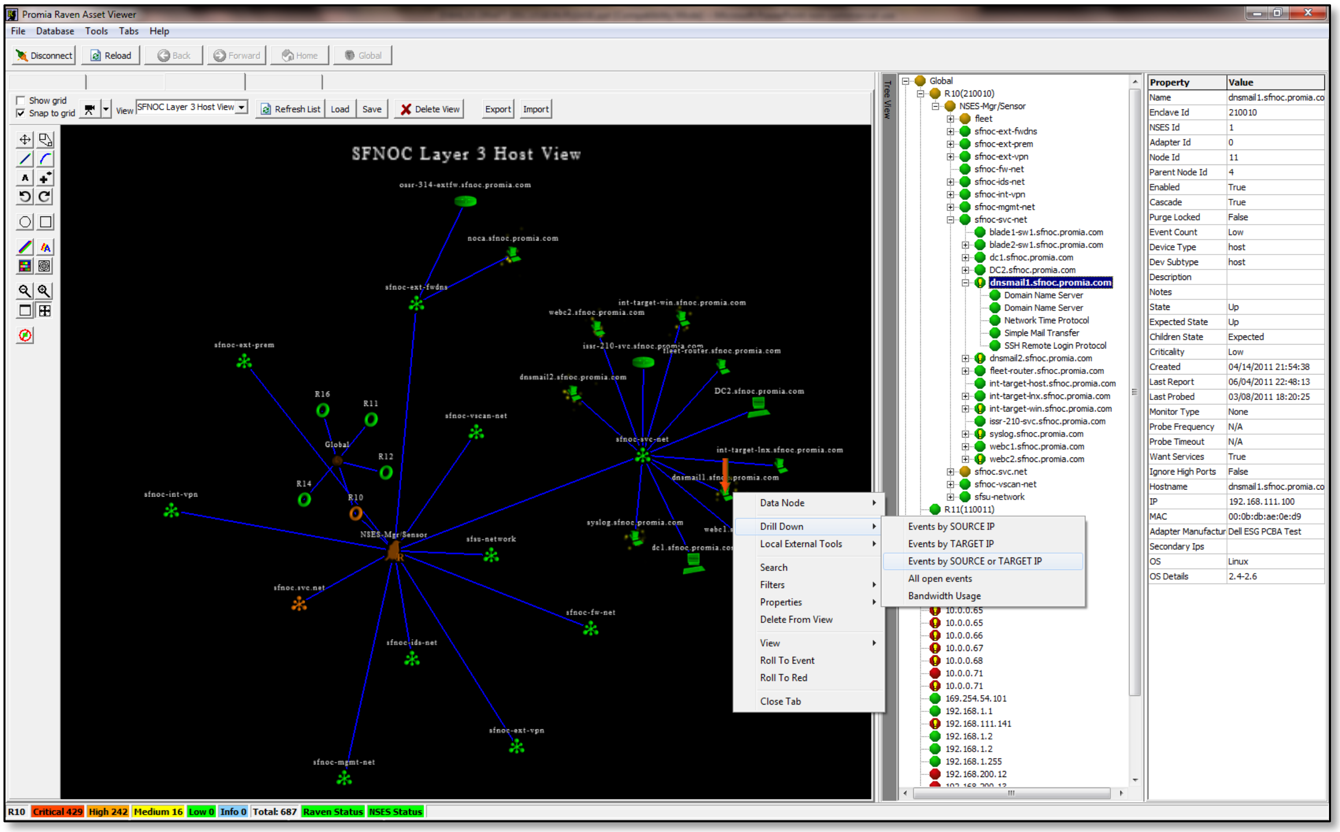
	State	Network Name	Last Observed Activity	Address Range of Hosts	# of Hosts	Incident Present?
⊟	●	ecrnoc	2010-12-07 23:51:14	130.212.0.0 - 130.212.0.255	0	No
	No Hosts Found.					
⊟	●	iornoc	2010-12-06 23:09:12	207.104.164.0 - 207.104.164.127	8	Yes

State	Child	Inc?	Crit	Host Name	IP	OS	Last Observed Activity	History	Launch Probe
●	●	Yes	2	207-104-164-121.ded.pacbell.net	207.104.164.121 (207-104-164-121.ded.pacbell.net)	Linux (2.6 (newer, 2))	2010-12-06 23:09:12	View	Probe
●	●	Yes	2	207-104-164-27.ded.pacbell.net	207.104.164.27 (207-104-164-27.ded.pacbell.net)	Linux (2.6? (barebone, rare!))	2010-10-28 20:59:30	View	Probe
●	●	No	2	207-104-164-122.ded.pacbell.net	207.104.164.122 (207-104-164-122.ded.pacbell.net)	Windows (2000 SP2+, XP SP1+ (seldom 98))	2010-10-20 22:28:40	View	Probe
●	●	No	2	207-104-164-1.ded.pacbell.net	207.104.164.1 (207-104-164-1.ded.pacbell.net)		2010-10-20 17:08:17	View	Probe

RAVEN Network Asset Viewer

Using the web interface, an operator can drill down into and close incidents, see different tactical status views of detected incidents, generate reports, manage the Promia RAVEN configuration, set up users and peer Promia RAVEN appliances, manage updates, and download the Asset Viewer installer.

The RAVEN also comes with the Promia Asset Viewer (AV) GUI, shown below, which presents a flexible, powerful, 3-dimensional, consolidated visualization of all assets and incidents on the monitored networks. The Asset Viewer shows versions and patch levels of node operating systems, device and application status, ports in use, and other related information. The AV enables an operator to navigate among multiple network segments being monitored by Promia NSES appliances, thus exposing the contextual relationship between those segments. The Asset Viewer provides a real-time tactical status view of the RAVEN incidents and the network's operational status.



View: SFNOC Layer 3 Host View

☐ Show grid
☑ Snap to grid

- Global
  - R10(210010)
    - NSES-Mgr/Sensor
      - fleet
      - sfnoc-ext-fwdns
      - sfnoc-ext-prem
      - sfnoc-ext-vpn
      - sfnoc-fw-net
      - sfnoc-ids-net
      - sfnoc-int-vpn
      - sfnoc-mgmt-net
      - sfnoc-svc-net
        - blade1-sw1.sfnoc.promia.com
        - blade2-sw1.sfnoc.promia.com
        - dc1.sfnoc.promia.com
        - DC2.sfnoc.promia.com
        - dnsmail1.sfnoc.promia.com
          - Domain Name Server
          - Domain Name Server
          - Network Time Protocol
          - Simple Mail Transfer
          - SSH Remote Login Protocol
        - dnsmail2.sfnoc.promia.com
        - fleet-router.sfnoc.promia.com
        - int-target-host.sfnoc.promia.com
        - int-target-lnx.sfnoc.promia.com
        - int-target-win.sfnoc.promia.com
        - issr-210-svc.sfnoc.promia.com
        - syslog.sfnoc.promia.com
        - webc1.sfnoc.promia.com
        - webc2.sfnoc.promia.com
      - sfnoc.svc.net
      - sfnoc-vscan-net
      - sfsu-network
  - R11(110011)
  - 10.0.0.65
  - 10.0.0.65
  - 10.0.0.66
  - 10.0.0.67
  - 10.0.0.68
  - 10.0.0.71
  - 10.0.0.71
  - 169.254.54.101
  - 192.168.1.1
  - 192.168.111.141
  - 192.168.1.2
  - 192.168.1.2
  - 192.168.1.255
  - 192.168.200.12

Property	Value
Name	dnsmail1.sfnoc.promia.co
Enclave Id	210010
NSES Id	1
Adapter Id	0
Node Id	11
Parent Node Id	4
Enabled	True
Cascade	True
Purge Locked	False
Event Count	Low
Device Type	host
Dev Subtype	host
Description	
Notes	
State	Up
Expected State	Up
Children State	Expected
Criticality	Low
Created	04/14/2011 21:54:38
Last Report	06/04/2011 22:48:13
Last Probed	03/08/2011 18:20:25
Monitor Type	None
Probe Frequency	N/A
Probe Timeout	N/A
Want Services	True
Ignore High Ports	False
Hostname	dnsmail1.sfnoc.promia.co
IP	192.168.111.100
MAC	00:0b:db:ae:0e:d9
Adapter Manufactur	Dell ESG PCBA Test
Secondary Ips	
OS	Linux
OS Details	2.4-2.6

R10 | Critical 429 | High 242 | Medium 16 | Low 0 | Info 0 | Total: 687 | Raven Status | NSES Status