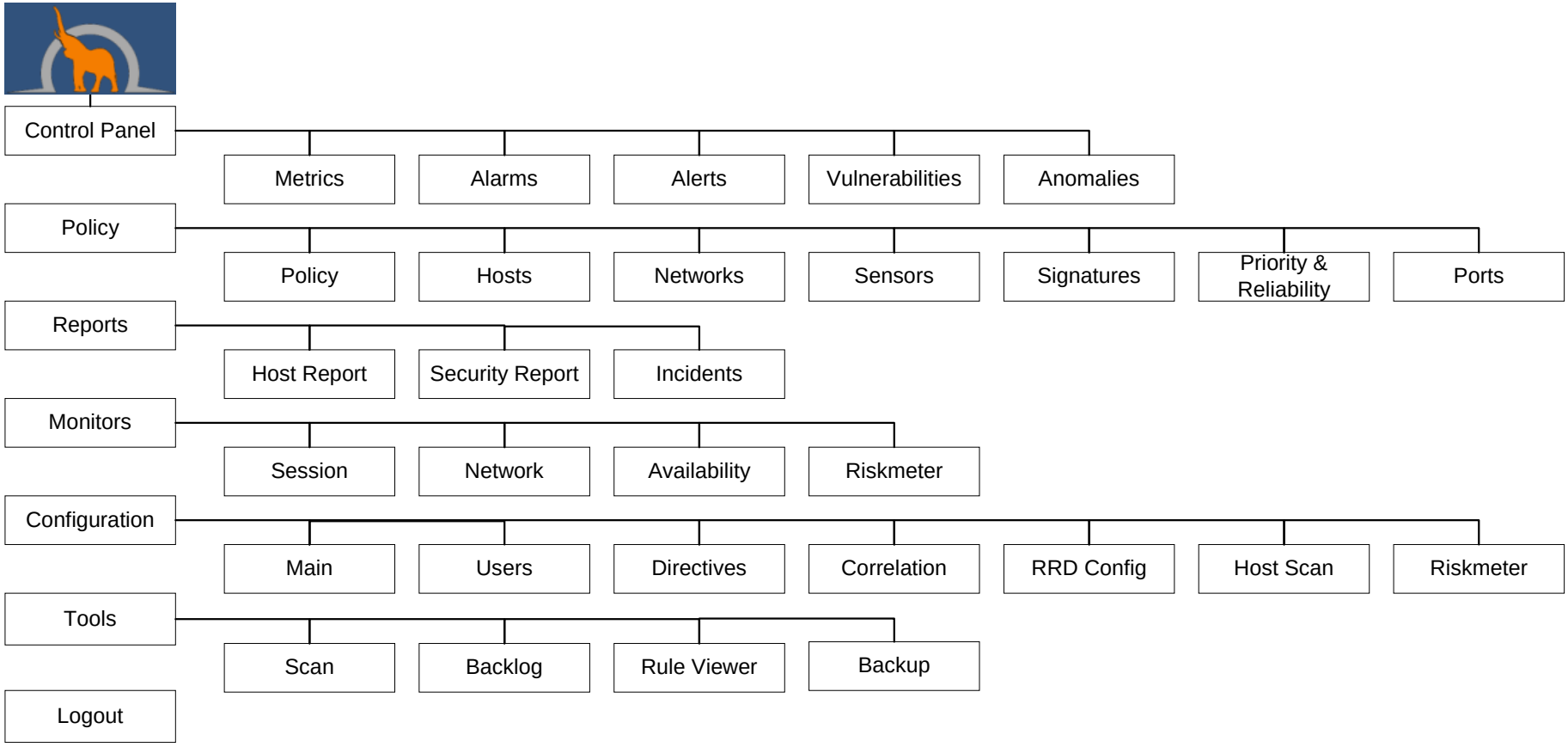
Open Source Security Information Management (OSSIM)

Overview

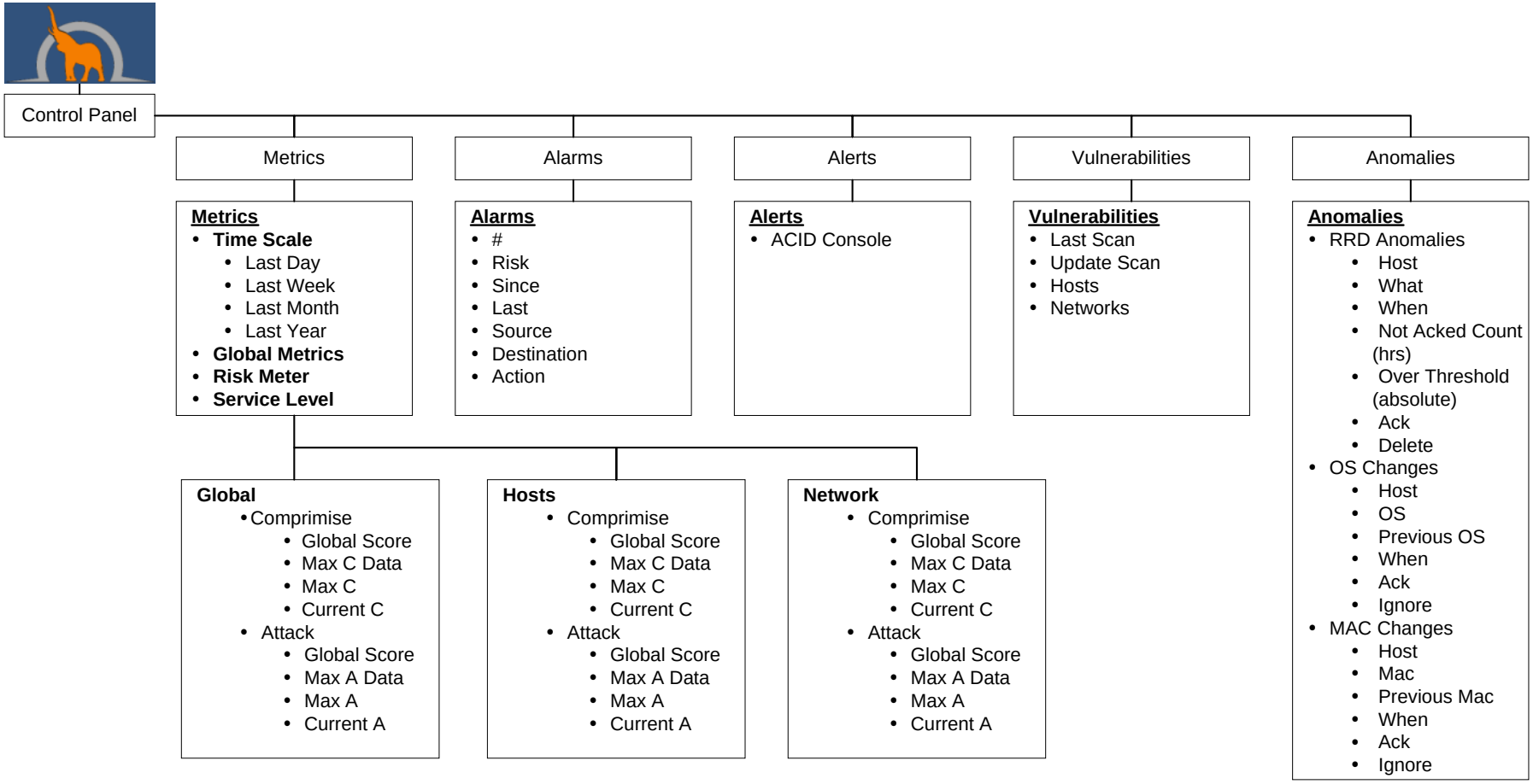
What OSSIM Does

- Monitors
  - Networks
  - Systems
- Reports
  - Attacks
  - Compromises
- Correlates compromises and attacks between various sensors to reduce false positives.
- Does not automatically block attacks.

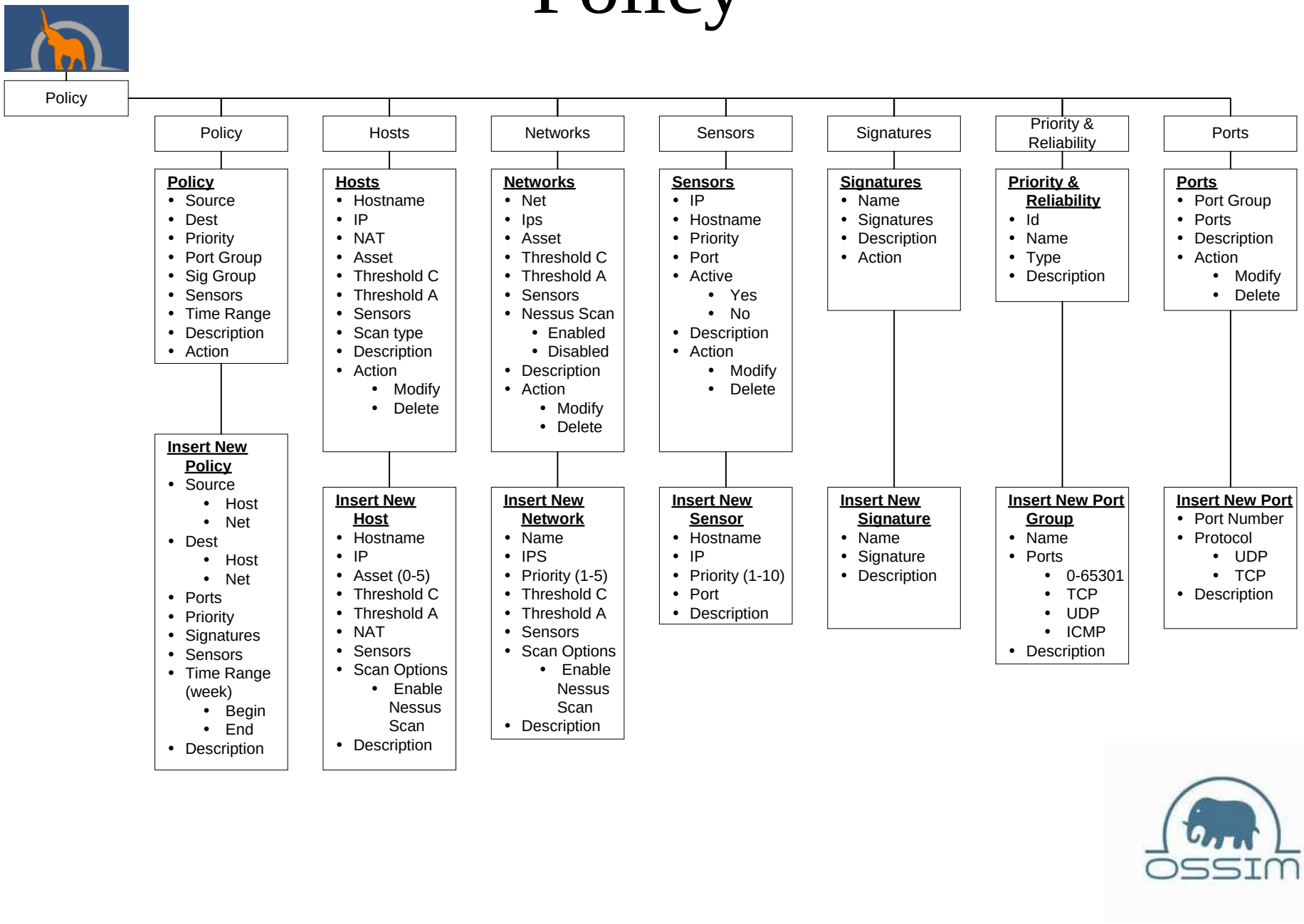
Components


Control Panel
Metrics
Alarms
Alerts
Vulnerabilities
Anomalies
Policy
Policy
Hosts
Networks
Sensors
Signatures
Priority & Reliability
Ports
Reports
Host Report
Security Report
Incidents
Monitors
Session
Network
Availability
Riskmeter
Configuration
Main
Users
Directives
Correlation
RRD Config
Host Scan
Riskmeter
Tools
Scan
Backlog
Rule Viewer
Backup
Logout

Control Panel



Policy

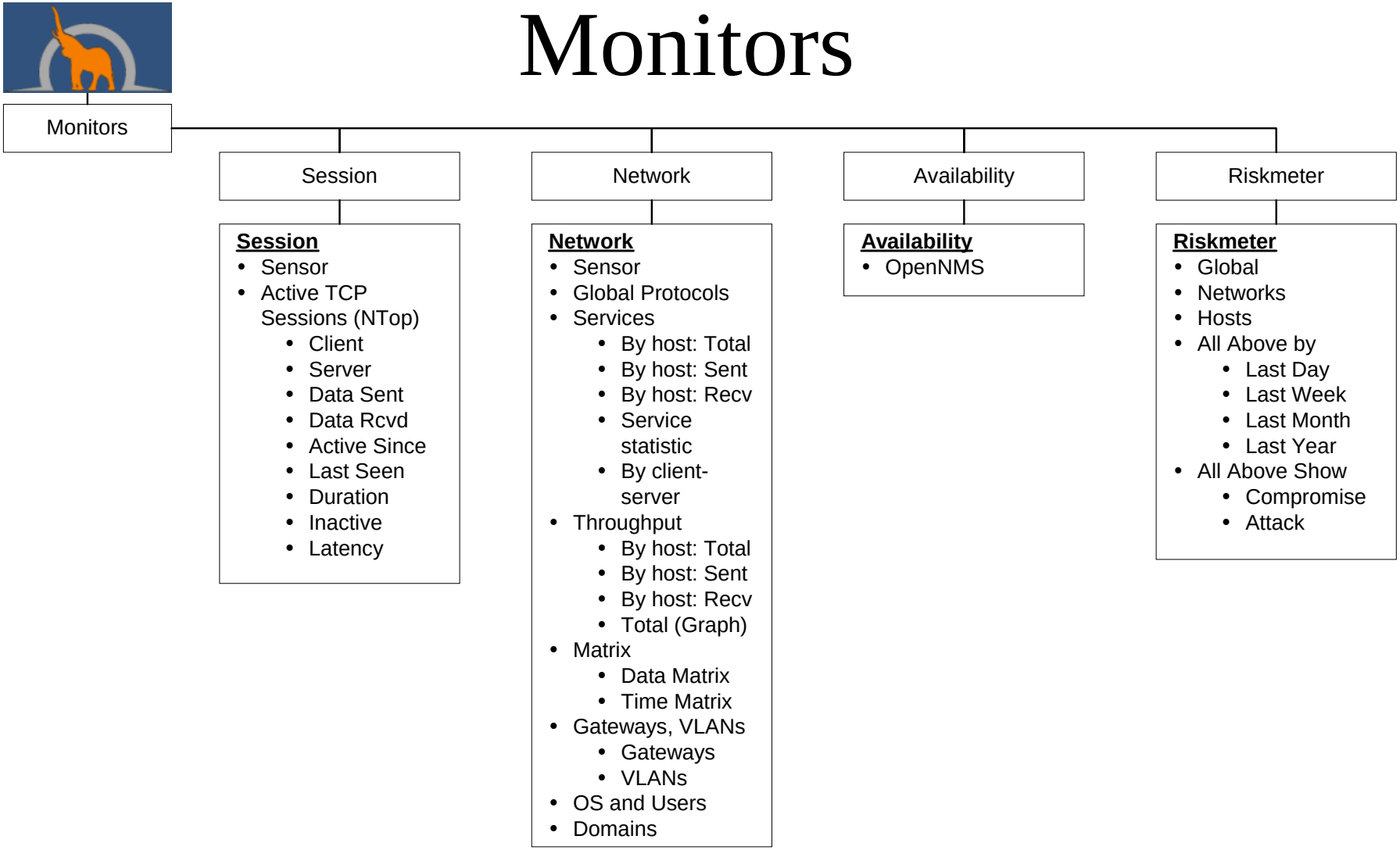

Policy
Policy
Hosts
Networks
Sensors
Signatures
Priority & Reliability
Ports
Policy
Source
Dest
Priority
Port Group
Sig Group
Sensors
Time Range
Description
Action
Insert New Policy
Source
Host
Net
Dest
Host
Net
Ports
Priority
Signatures
Sensors
Time Range (week)
Begin
End
Description
Hosts
Hostname
IP
NAT
Asset
Threshold C
Threshold A
Sensors
Scan type
Description
Action
Modify
Delete
Insert New Host
Hostname
IP
Asset (0-5)
Threshold C
Threshold A
NAT
Sensors
Scan Options
Enable Nessus Scan
Description
Networks
Net
Ips
Asset
Threshold C
Threshold A
Sensors
Nessus Scan
Enabled
Disabled
Description
Action
Modify
Delete
Insert New Network
Name
IPS
Priority (1-5)
Threshold C
Threshold A
Sensors
Scan Options
Enable Nessus Scan
Description
Sensors
IP
Hostname
Priority
Port
Active
Yes
No
Description
Action
Modify
Delete
Insert New Sensor
Hostname
IP
Priority (1-10)
Port
Description
Signatures
Name
Signatures
Description
Action
Insert New Signature
Name
Signature
Description
Priority & Reliability
Id
Name
Type
Description
Insert New Port Group
Name
Ports
0-65301
TCP
UDP
ICMP
Description
Ports
Port Group
Ports
Description
Action
Modify
Delete
Insert New Port
Port Number
Protocol
UDP
TCP
Description

Reports

Reports

- Host Report
  - **Host Report**
    - Inventory
    - Metrics
    - Alarms
      - Source or Dest
      - Source
      - Destination
    - Alerts
      - Main
      - Src Unique alerts
      - Dst Unique alerts
    - Vulnerabilites
      - Vulnmeter
      - Security Problems
    - Usage
    - Anomalies
- Security Report
  - **Security Report**
    - Top Attacked Hosts
    - Top Attacker Hosts
    - Top Alerts Received
    - Top Alerts by Risk
    - Top Destination Ports
    - Top Availability
    - All
- Incidents
  - **Filter**
    - Type
      - All
      - Alarm
      - Metric
    - Title
    - In Charge
    - Status
      - All
      - Opened
      - Closed
    - Priority
      - All
      - High
      - Medium
      - Low
    - Filter
      - OK

Monitors

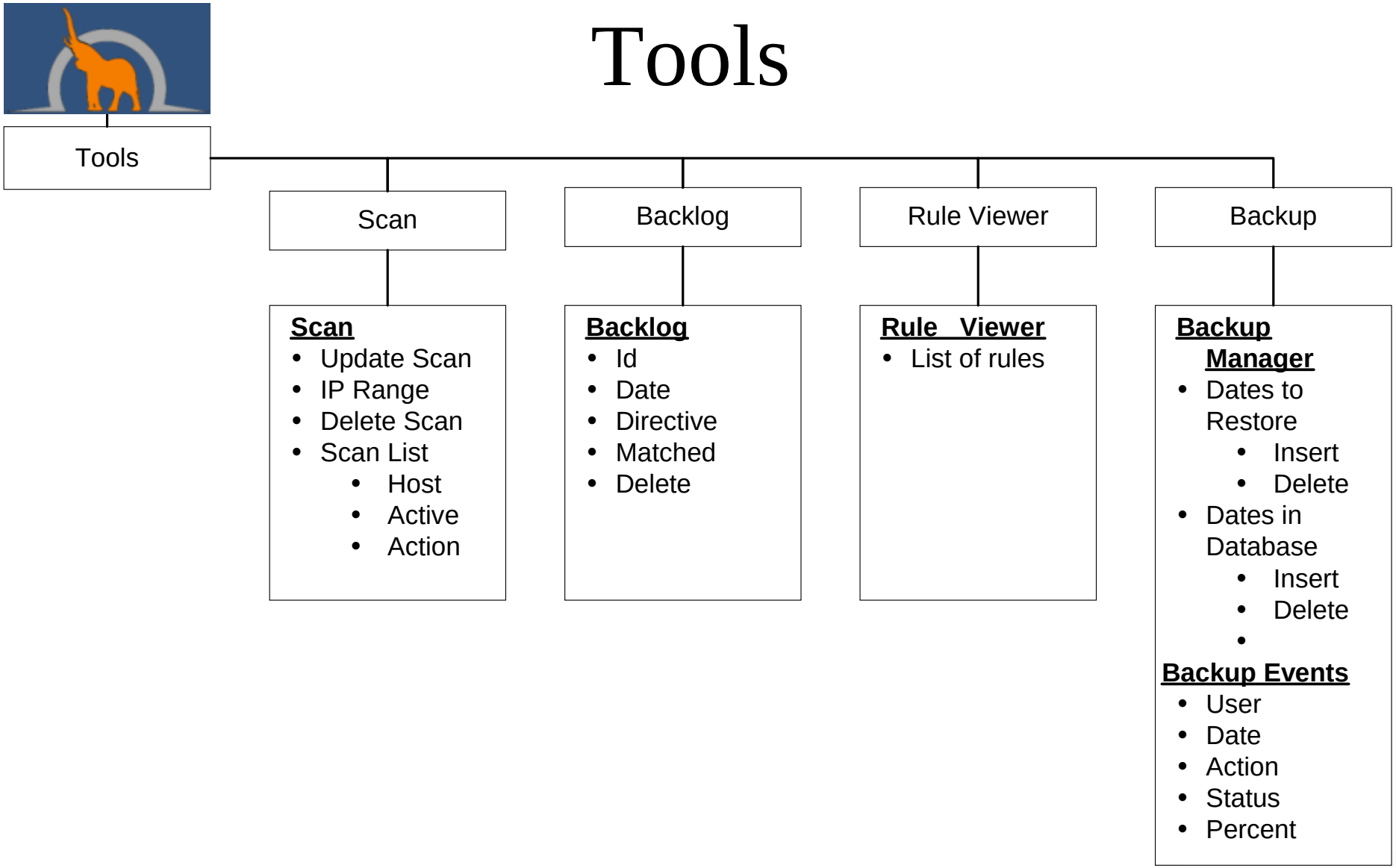

Monitors
Session
Network
Availability
Riskmeter
Session
Sensor
Active TCP Sessions (NTop)
Client
Server
Data Sent
Data Rcvd
Active Since
Last Seen
Duration
Inactive
Latency
Network
Sensor
Global Protocols
Services
By host: Total
By host: Sent
By host: Recv
Service statistic
By client-server
Throughput
By host: Total
By host: Sent
By host: Recv
Total (Graph)
Matrix
Data Matrix
Time Matrix
Gateways, VLANs
Gateways
VLANs
OS and Users
Domains
Availability
OpenNMS
Riskmeter
Global
Networks
Hosts
All Above by
Last Day
Last Week
Last Month
Last Year
All Above Show
Compromise
Attack

Configuration

Configuration

- **Main**
  - **Main Configuration**
    - Reload server structures
      - RELOAD ALL
      - Reload policies
      - Reload hosts
      - Reload nets
      - Reload sensors
- **Users**
  - **Users**
    - Login
    - Name
    - Password
    - Actions
      - Change Password
      - Update
      - Delete
  - **Insert New User**
    - User login
    - User full name
    - Enter password
    - Re-enter password
    - Allowed nets
  - **Permissions**
    - **Control Panel**
      - Metrics
      - Alarms
      - Alerts
      - Vulnerabilities
      - Anomalies
    - **Policy**
      - Policy
      - Hosts
      - Networks
      - Sensors
      - Policy & Signatures
      - Priority & Reliability
      - Ports
    - **Reports**
      - HostReport
      - SecurityReport
      - Incidents
    - **Monitors**
      - Session
      - Network
      - Availability
      - Riskmeter
    - **Configuration**
      - Main
      - Users
      - Directives
      - Correlation
      - RRD Config
      - Host Scan
      - Riskmeter
    - **Tools**
      - Scan
      - Backlog
      - RuleViewer
      - Backup
- **Directives**
  - **Directives Editor**
    - Directives
    - ID
    - Name
    - Edit
      - Priority #
      - Reliability #
- **Correlation**
  - **Modify RRD Config**
    - Global
      - Attribute
      - Threshold
      - Priority
      - Alpha
      - Beta
      - Persistence
    - Insert IP
      - Attribute
      - Threshold
      - Priority
      - Alpha
      - Beta
      - Persistence
- **RRD Config**
  - **Correlation (Plugin Reference)**
    - Plugin id
    - Plugin sid
    - Reference id
    - Reference sid
- **Host Scan**
  - **Insert New Host Scan Configuration**
    - Host IP
    - Plugin id
      - NMAP
      - Nessus
- **Riskmeter**
  - **RiskMeter Configuration**
    - Recovery level
    - Default threshold
    - Graph default threshold
    - Left Bar length
    - Right Bar length

Tools


Tools
Scan
Backlog
Rule Viewer
Backup
Scan
• Update Scan
• IP Range
• Delete Scan
• Scan List
• Host
• Active
• Action
Backlog
• Id
• Date
• Directive
• Matched
• Delete
Rule Viewer
• List of rules
Backup Manager
• Dates to Restore
• Insert
• Delete
• Dates in Database
• Insert
• Delete
Backup Events
• User
• Date
• Action
• Status
• Percent