Framework for Responding to Network System Events:

Autonomic, policy-based response

Scott A. Miller
samiller@lanl.gov
samiller@lanl.doe.sgov.gov
Senior System Architect

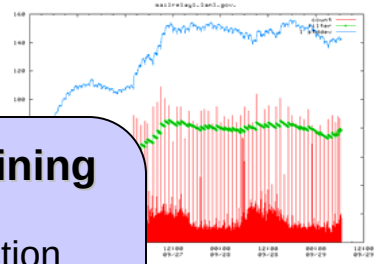
Advanced Computing Solutions Program
Los Alamos National Laboratory

LAUR 08-2731
Unclassified unlimited release
Name/Org: LANL ACS PO.
Date: 28 April 2008

Los Alamos
NATIONAL LABORATORY
EST. 1943

The Threat- Resilient Network

A system of integrated LANL technologies



Real-Time Data Mining

Parallel Data Collection
Change Detection
Malware Analysis
Fingerprinting

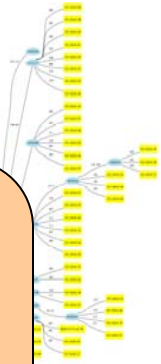
Full-Spectrum Security

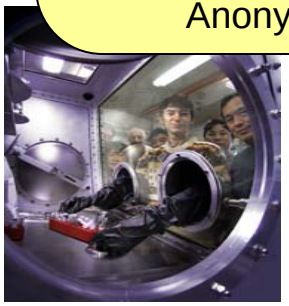
Global Virtual Vault
Role-based Execution
Predictive Modeling
Red Teaming
Anonymization

Threat-Resilient Network

Active Response

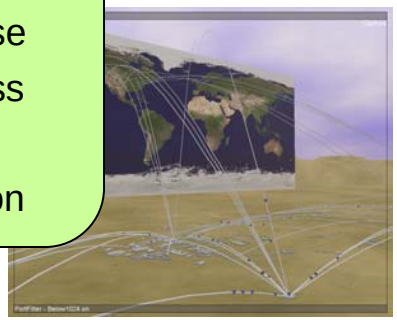
Quarantine
Network Reconfiguration
Intelligence Analysis
Active Attribution



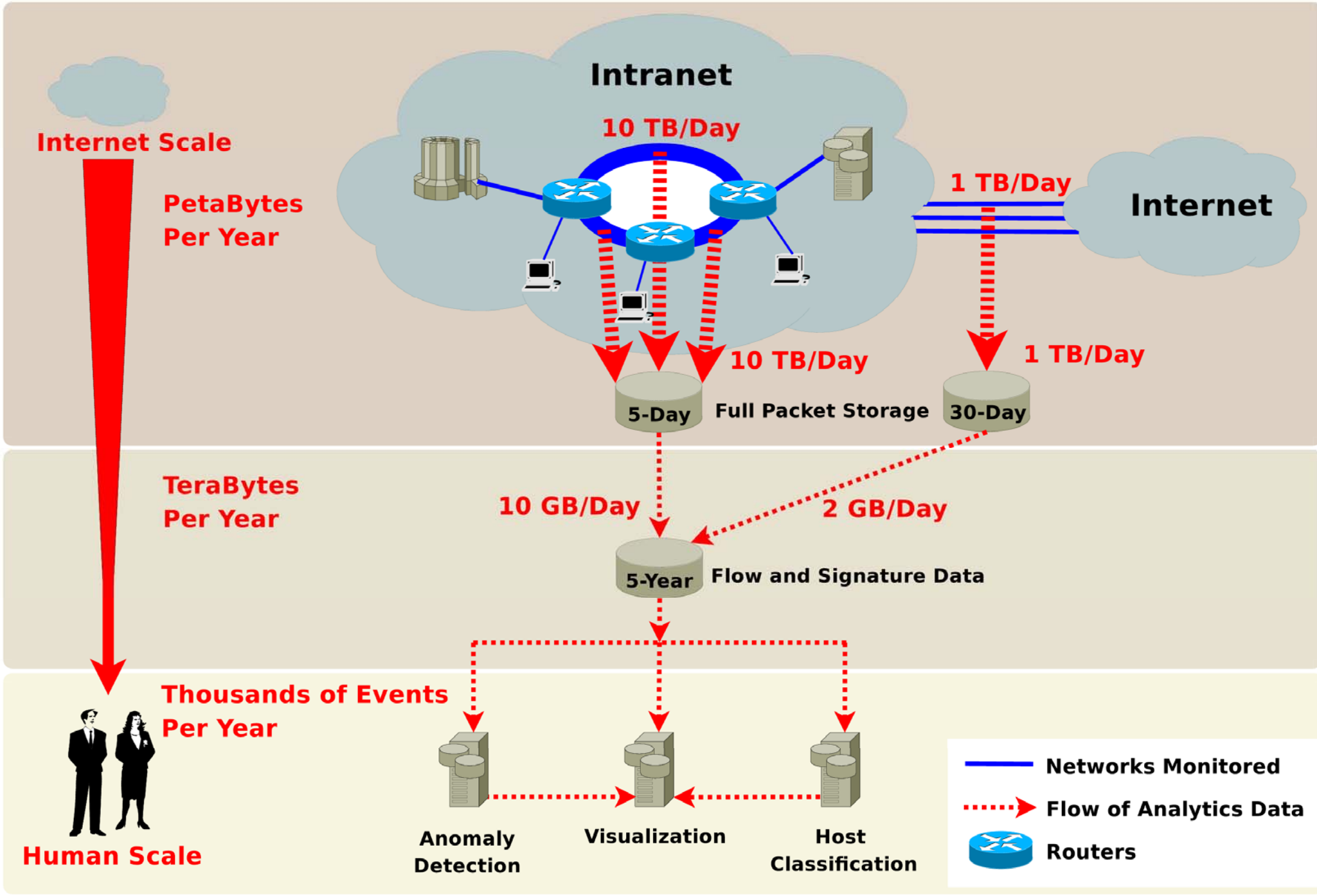


Knowledge Synthesis

Rule-Based Response
Situational Awareness
Visualization
Knowledge Integration



Los Alamos NATIONAL LABORATORY EST. 1943


Internet Scale
PetaBytes
Per Year
Intranet
10 TB/Day
1 TB/Day
Internet
10 TB/Day
1 TB/Day
5-Day
Full Packet Storage
30-Day
TeraBytes
Per Year
10 GB/Day
2 GB/Day
5-Year
Flow and Signature Data
Thousands of Events
Per Year
Human Scale
Anomaly
Detection
Visualization
Host
Classification
Networks Monitored
Flow of Analytics Data
Routers

Real-Time Automated Reponses

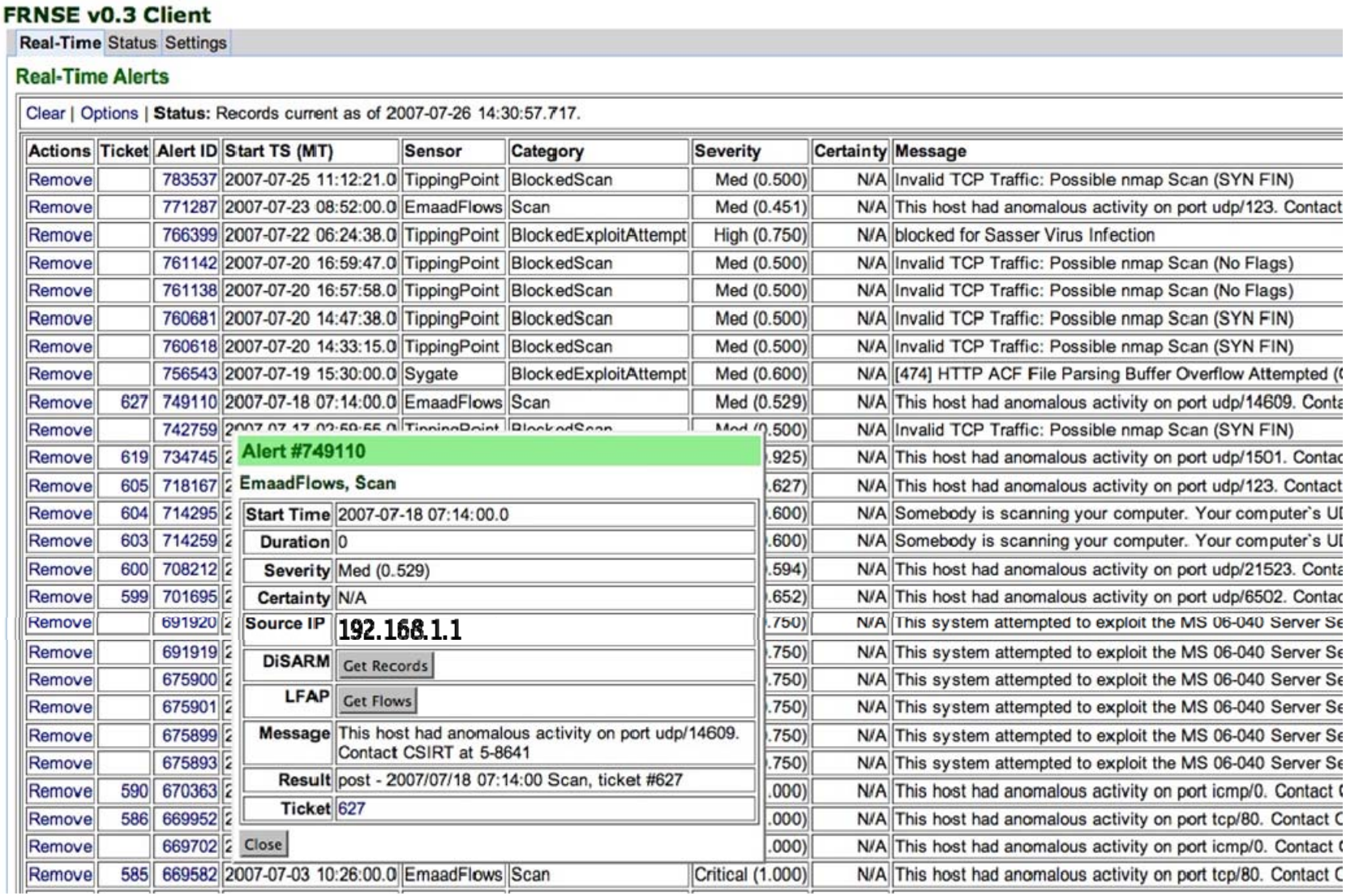
- Framework for Responding to Network Security Events (FRNSE)
  - Collects and correlates real-time events from diverse network and host sensors
    - Flow-based anomaly detectors, IDS/IPS, honeypots, e-mail anomalies, etc.
  - Policy and anomaly detection engines controlling multiple real-time responses
    - Internal quarantine, perimeter changes, analyst tasking, etc.
- Real-time scan detection
  - Using flow-accounting data
    - LFAP, sFlow, Netflow, etc.
    - Wide-spread coverage without new sensor deployment
- Real-time isolation from network
  - Turn-off Ethernet port
    - Using SNMP control
    - Multi-vendor support in networks
  - RADIUS-based MAC authentication
    - Worked with multiple vendors to implement
- Can preventatively quarantine vulnerable systems before they are infected
  - Based on network vulnerability scanning results

FRNSE Goals

- Improve reaction time, accuracy, efficiency
- Reduce operational costs via automation
- Aggregate all sensor information from all sources
- Provide a unified risk/severity space for interpreting information
- Improve detection accuracy by correlating among and across sensors

Enable the analyst with a common view of sensors and responses

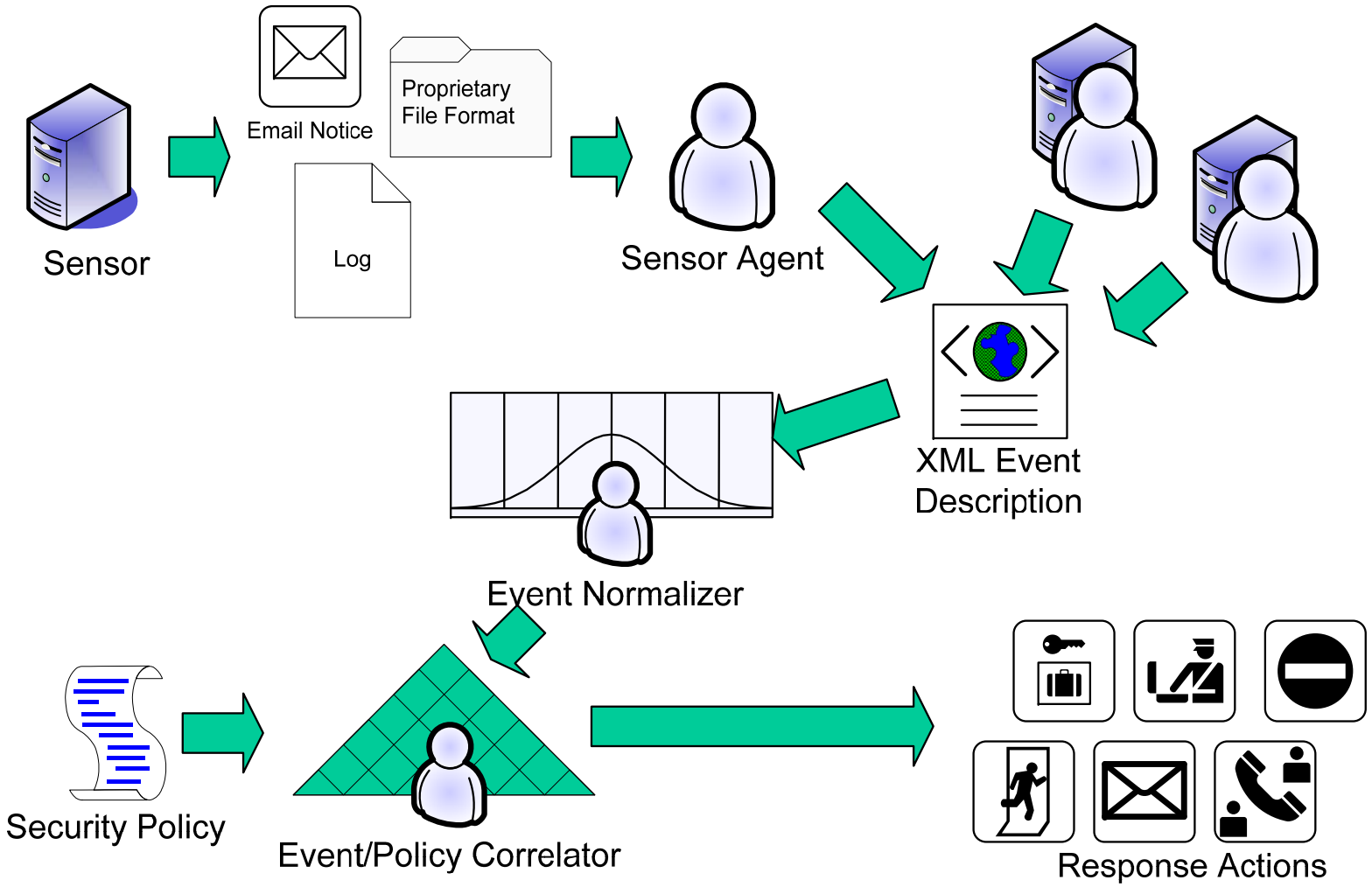
FRNSE Interface



FRNSE vs. Conventional SIM/SEM

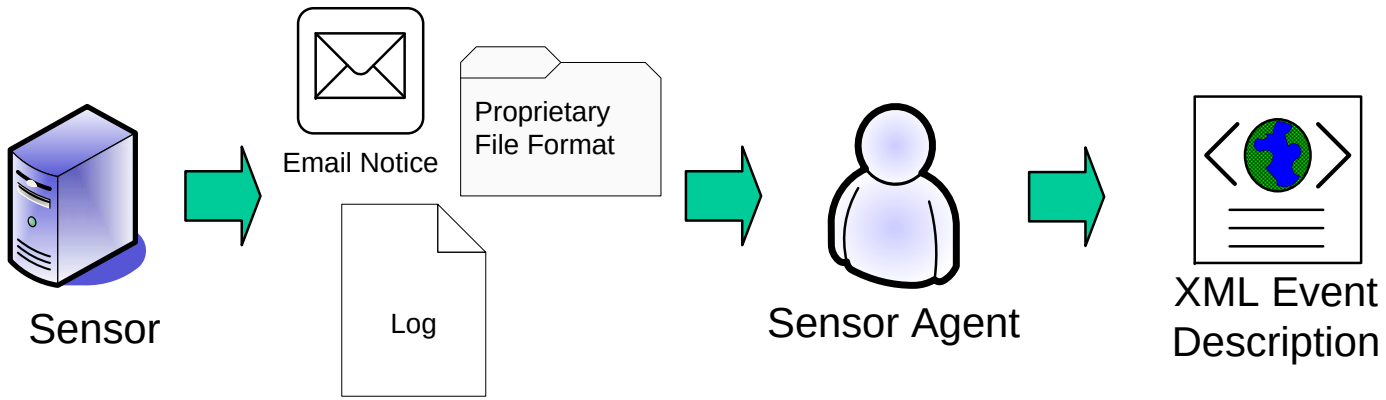
- Scalable, user-extensible
- XML event format, SQL storage schema
- Supports strongly heterogeneous networks
- Multi-vendor support
- Data interfaces for GUI and CLI

FRNSE Structure



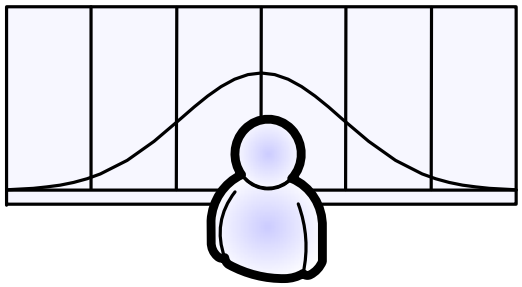
Sensor Agents

- One agent instance per sensor
- Event summary in uniform XML Event Description
  - Enables comparison
  - Enables direct analysis by external tools
  - Default schema
    - Time
    - Severity
    - Event description
    - Event Class
    - Sensor index/reference
    - Analyst description



Event Normalizer

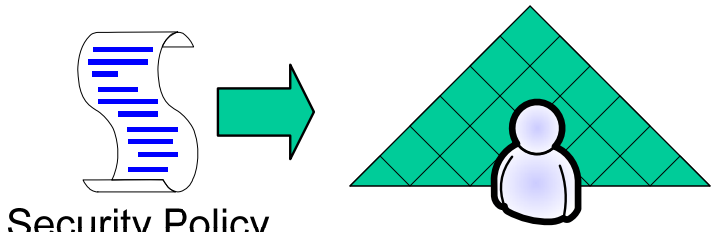
- Sensor information is kept ‘raw’
  - Allows reference to original data
  - Abstracts interface from data
- Agent normalizes severity from 0.0-1.0
  - Incorporates both severity and confidence
  - Captures analyst feedback
  - Manages multiple sensors and multiple sensor instances



Event Normalizer

Policy and Event Correlator

- Correlation is against policy and across sensors
- Written in a full-featured language (Python)
- Enables for technical implementation of complex policy
  - “If a machine has not been properly patched, quarantine the host”
  - “If a machine is running an OS version that is vulnerable to the exploit attempt just detected, increase the response.”
  - “If it is not during normal business hours or the analyst ticket queue is long, decrease the automated response threshold.”



Response Actions

- Side-effect: Creates a uniform interface to response actions
- Integration with analyst workflow
  - Automatic ticket generation
  - Includes context for rapid analyst understanding
- Integration with response capabilities
  - Traffic filtering, switch blocking, forensics collection, account disablement
  - Implementation reflects an a priori consideration for minimizing impact

Response Actions

FRNSE Production Results

- 11 sensor agents, 12 instances
  - AirDefense
  - Sygate
  - TippingPoint
  - Nepenthes
  - Snort
  - Other internal sensors
- In 2007:
  - 919,737 alerts handled by FRNSE
  - 283,192 automatic firewall blocks
  - 2,293 analyst tickets generated
  - 179 automatic internal host quarantine events

Of 919,737 alerts generated in 2007, 99.75% were directly addressed by technical implementation of policy and required no analyst intervention.

Summary

Multi-vendor sensor aggregation and response automation is possible and serves as a force-multiplier for analyst operations.

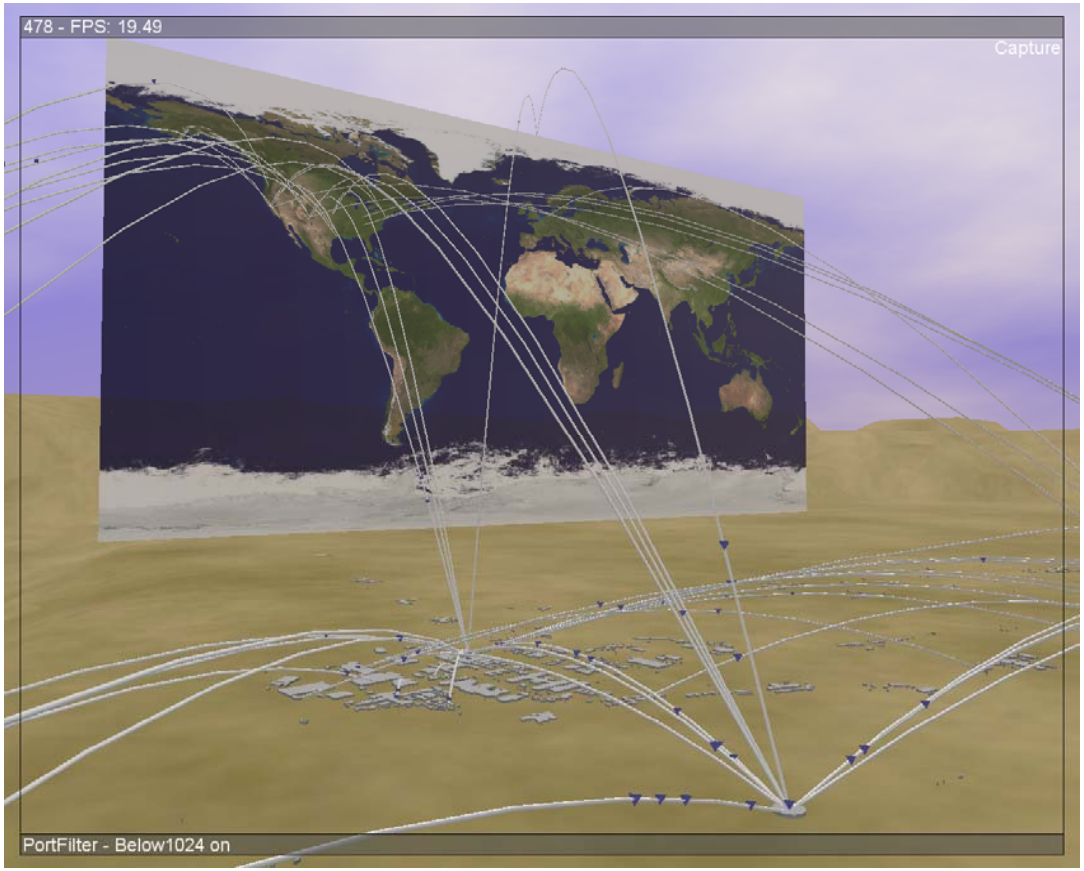
Future work: The Threat Resilient Network.

For more information:
samiller@lanl.gov
samiller@lanl.doe.sgov.gov

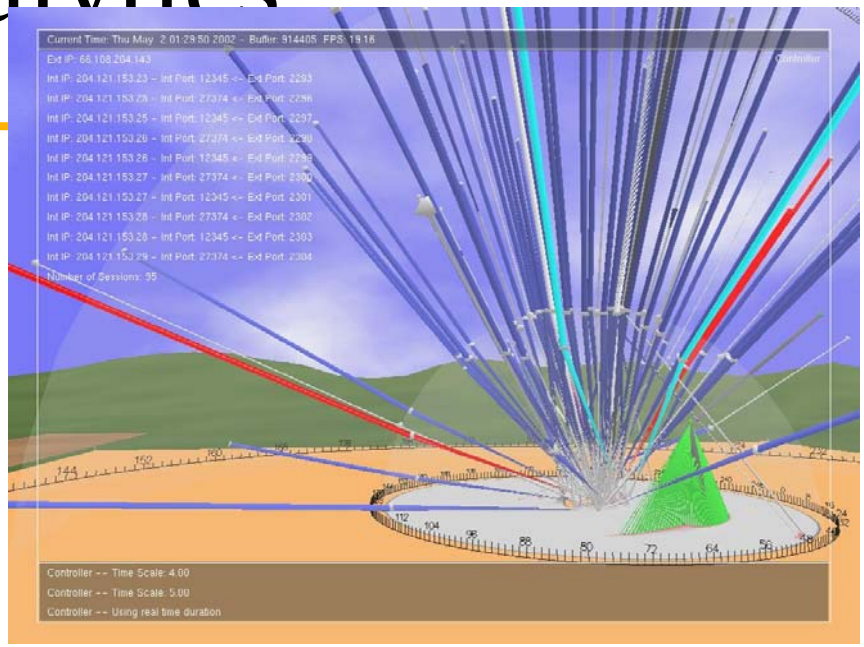
Los Alamos NATIONAL LABORATORY EST. 1943

Extra Slides

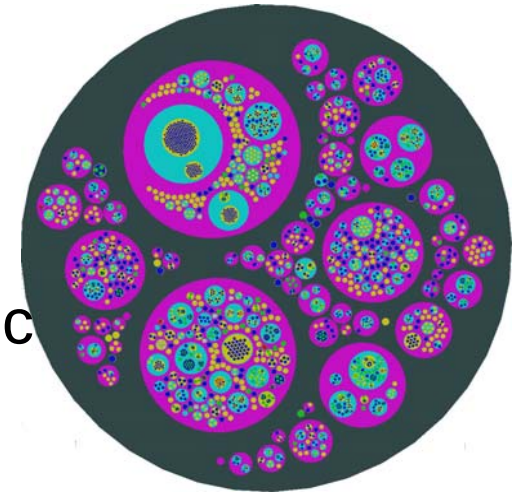
Real-time Visual Analytics



Geo-spatial representation of network traffic



Coordinate-space visualization of network scans



Representation of domain name hierarchies

Los Alamos NATIONAL LABORATORY EST. 1943

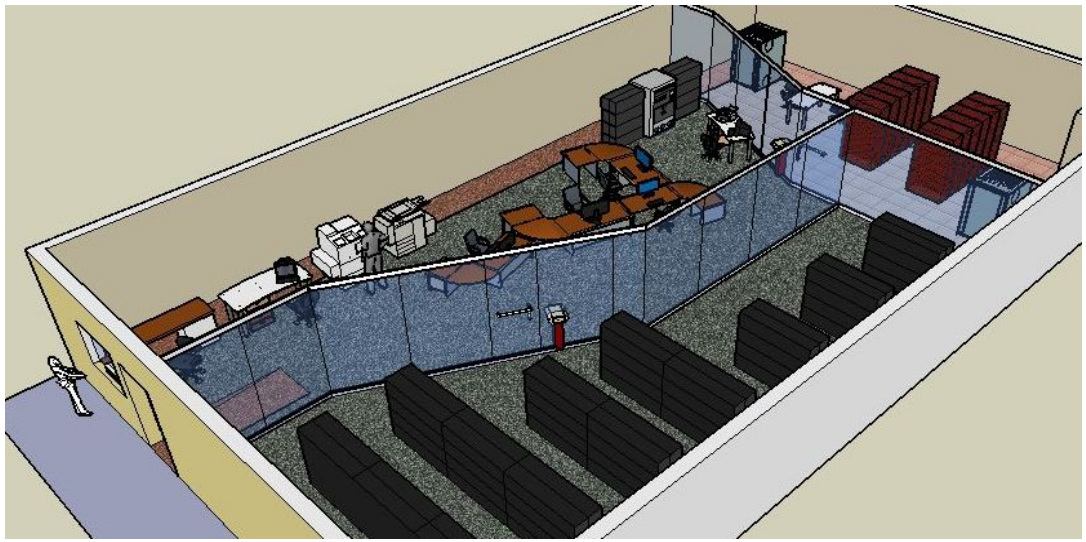
Global Virtual Vault System Elements

Nvidia Quadraplex rendering servers and VirtualGL for high-performance graphics.

LANL Red Team found three 0-day vulnerabilities in terminal services.

Secure, bandwidth-limited printing.

Library & service center for physical media & paper. Consolidate high-risk information-handling activities.



Los Alamos NATIONAL LABORATORY EST. 1943