enterasys® Secure Networks™

"There is nothing more important than our customers"

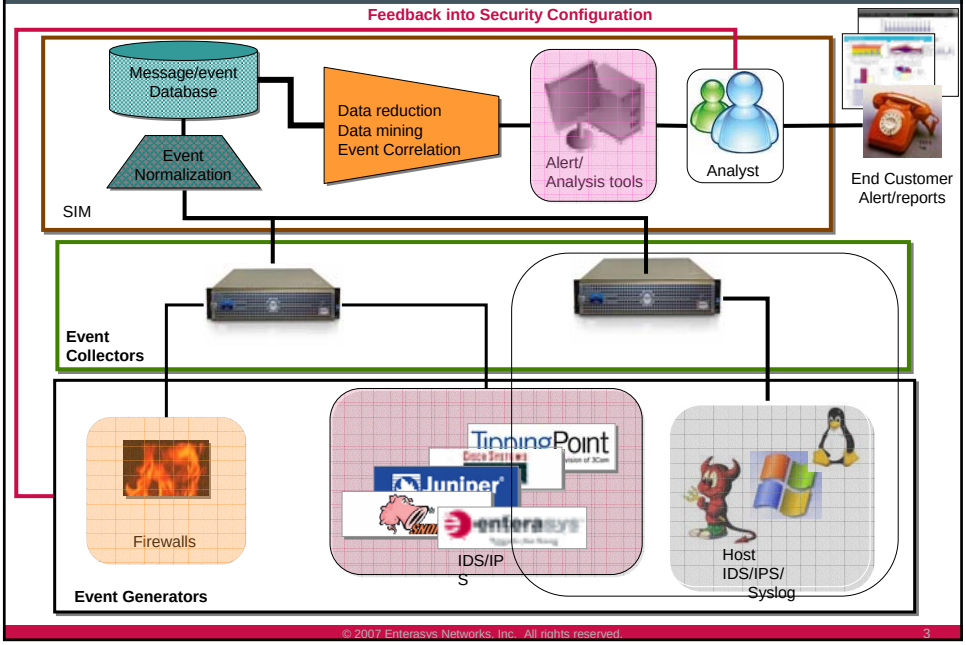
Introduction to Security Information Management

Agenda

enterasys® Secure Networks™

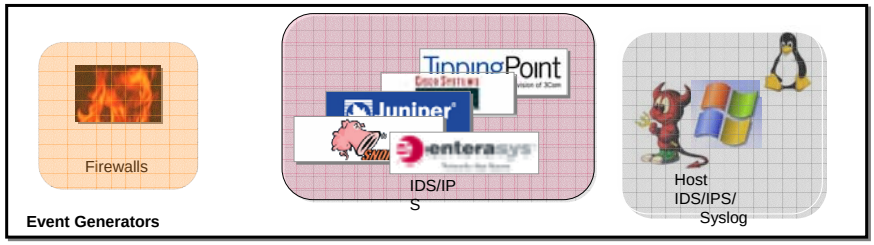
- The Flood - an overview of the problem space
- The Solution - what a Security Event Manager does for you
- The Benefits - why you should consider deploying a Security Event Manager

SIM System Logical Schematic



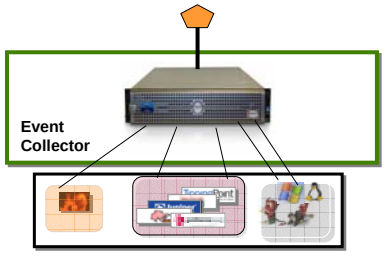
Event Generator Characteristics

- Amalgamation of different equipment from different vendors, performing different functions.
- **Current methodology - monitor everything separately**
  - Time consuming
  - Error prone
  - Does not correlate related events
  - Nobody really does it in the 'real word'; no time…
- No standards exist for the presentation of data
  - Manually need to learn and understand these formats ~or~
  - Need to roll your own data normalization tools



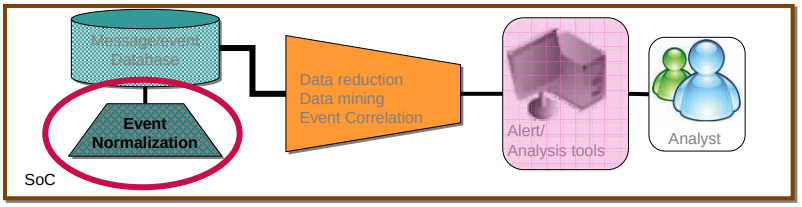
Event Collector Characteristics

- Key for scaling of SIM to serve thousands of sensors
- Aggregates many flows to a single flow
- May be deployed within SIM or as customer premise equipment
- Performs buffering for slow (remote) links to avoid data loss and over-utilization of bandwidth; also buffers data in event of link loss
- Performs VPN and other encryption services as necessary



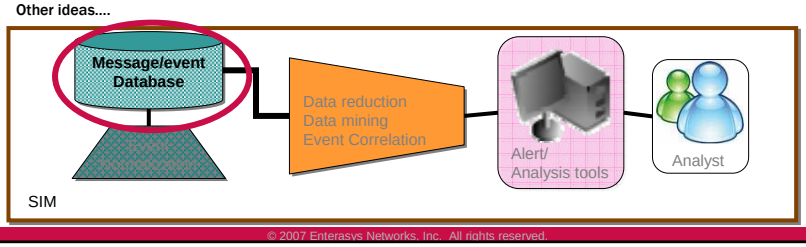
SIM - Event Normalization Characteristics

- Collects data in various vendor specific formats
- Modifies data for storage in common format specific to database and datamining
- MAY preserve original format also (to be stored in database) to allow for 'drill down' with vendor specific tools, as launched in conjunction with Alert/Analysis tools



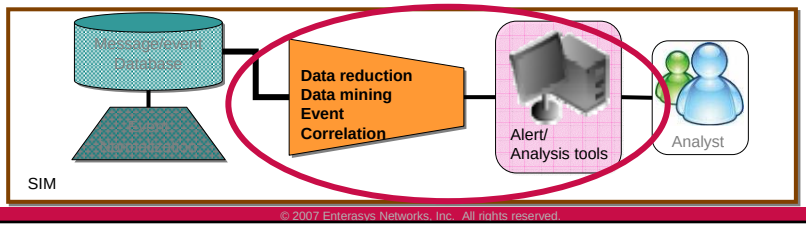
SIM - Message/Event Database

- Stores **all** events, captured packets, etc in normalized format
- More than one database may exist - **Example:** support for specific proprietary databases for 'drill down'
- Must store all events and captured packets for forensics and 'session replay' purposes
- Must be massive in terms of capacity - store events for at least 1 week 'online'; not practical to keep everything online forever.
- Must be redundant - RAID recommended
- Must have well thought out and specific data retention policy that customers understand; **Examples**:
  - Historical data out to tape or DVD after N days
  - Only header information preserved, not packet data
  - Key data for serious event against customer X is specifically given on DVD, and digitally signed to preserve data integrity and evidence trail
  - Dump of all customer data delivered on DVD(s) on monthly basis
  - Other ideas....



SIM - Event Data Processing

- Prioritize key events; **example:** attack on Exchange server is more important than attack on receptionist PC
- Generate alerts based on well-known events or pre-defined conditions; **example:** SQL Injection exploit, well known worm such as Blaster
- Correlate events; **examples:**
  - Host based IDS detects malformed URL, Network based IDS detects same malformed URL
  - Brute force login attempts attempted from IP address 193.21.67.59 to multiple host computers
- Eliminate irrelevant events; **example:** ping sweeps of your IP address range that don't correlate to an actual attack

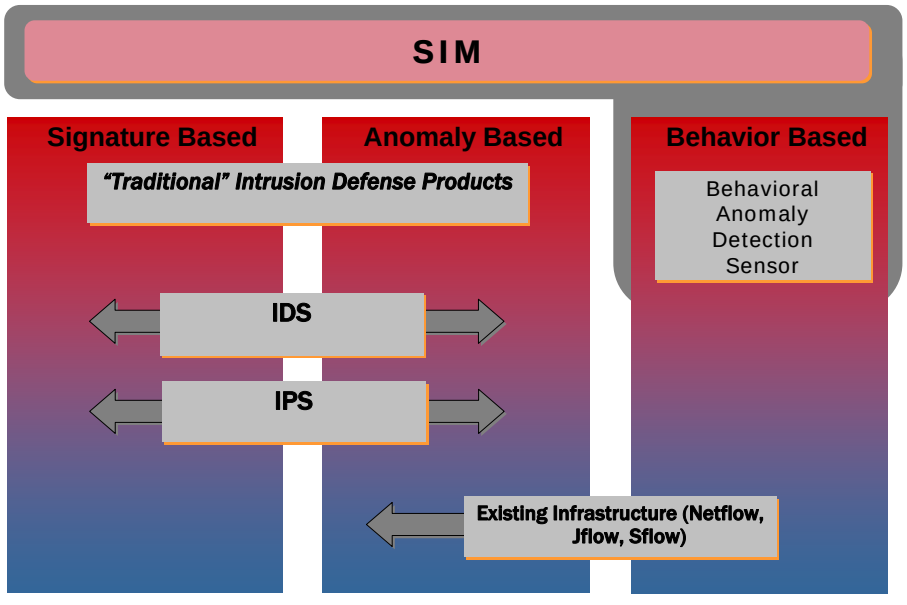


Why Data Reduction is Key…

- Typical *nix machine has more than 20 log files which may require monitoring
  - This number **does not count applications!**
- For more than a few servers, manual log file analysis just does not scale:
  - 20 Logs * 400 Servers = 8,000 individual log files
  - Each log file has hundreds of lines per day (Assume 200)
  - 8,000 * 200 = **1,600,000 lines to analyze per day**
- Different devices have different log file formats, making analysis more difficult
- Manual analysis is tedious
  - Probability of errors is higher

Manual log file analysis does not scale from a human sense

Different Types of Data To Be Collected



Helping to Eliminate Data Overload…

- Typical IDS in mid-sized deployment will generate 100,000 events per day
  - Only if well tuned
- Multiple monitored devices will generate alerts for a single event
  - Duplication of data = more work
- For each event…
  - › The analyst must prioritize the events based on attack type and the 'value' of the asset being attacked – ***continuous, on-going process***
  - › The analyst must verify if the attack was valid when considered in the context of the asset being attacked – in other words, was the end station vulnerable to the specific attack – ***3 minutes***
  - › The analyst must determine if the attack was successful – ***10 minutes***
  - › The analyst must correlate events from compromised systems (i.e. backdoor activity) with the events preceding the attack – ***15 minutes***
  - ***Total time = approximately 18 minutes***

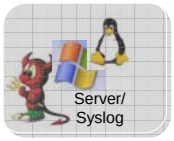
Data Reduction through SIM

- A SIM:
  - Automatically groups related events together
  - Prioritizes events based on **asset value** and **lethality of attack**
    - › If the asset is high value or the attack particularly lethal it's seen by analyst first
  - Considers how 'reliable' the 'reporter' is
    - › A well tuned IDS is considered more reliable than a poorly tuned instance of Snort
  - Considers the relevance of the attack against the target
    - › Attacking an Apache server with an attack designed to compromise Microsoft IIS won't work so it's discounted and given low priority
- **SIM dramatically reduces the number of events that the analyst must see and**

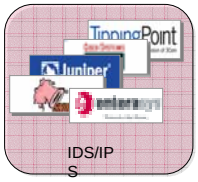
Many Data Sources, Many Data Formats…

- **Nobody can analyze this much data…**

- Intrusion Detection Systems
  - Generates thousands of events, overwhelming security analysts
  - SIM correlates/aggregates IDS events, from multiple sensors automatically
  - Enterasys DSCC supports third-party products, leveraging existing investment
- Syslog from servers and devices can be consumed
  - Can correlate events from IDS with syslog events
  - Support for wide variety of applications and operating systems
- Firewall Events can be consumed
- Network Access Control Events can be consumed
  - Gives extra information about attacker



Network access Control



The SIM Data Flow to Analyst Scalability

One 'Offense' Post Data Reduction for analyst response

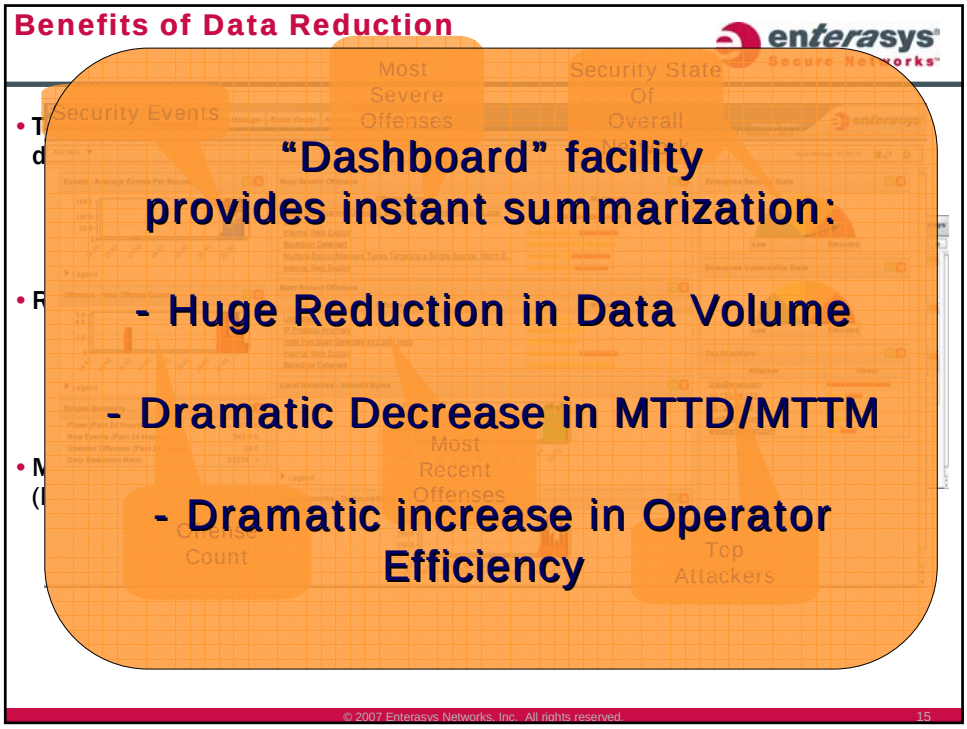
Benefit:

Analyst need only look at 1 Offense, not 193 discrete events; Analyst productivity is improved

6 Event Categories, 193 events summarized Automatically!

Behavioral Anomaly Detection

Benefits of Data Reduction



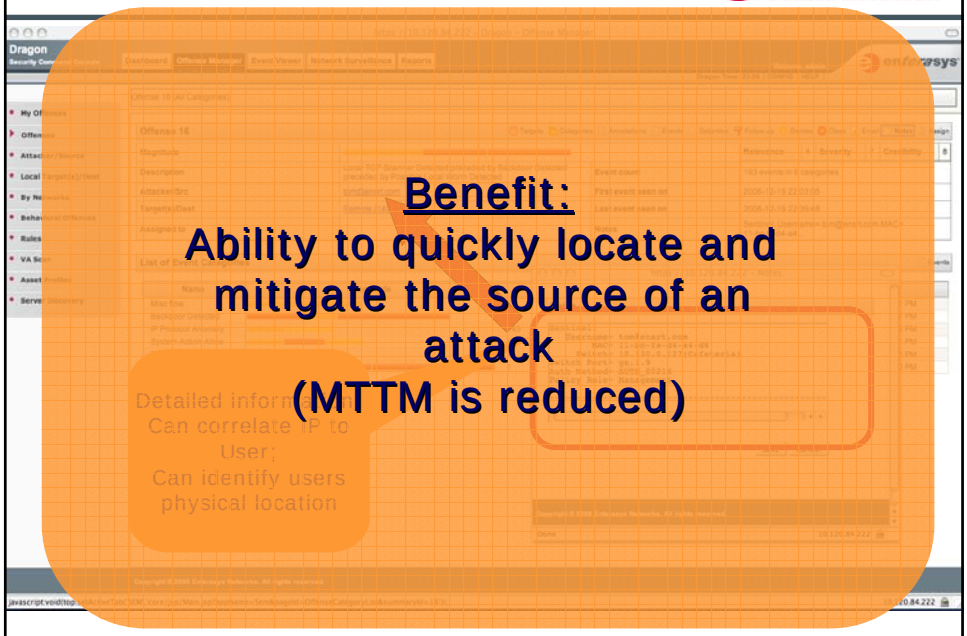
"Dashboard" facility provides instant summarization:

- Huge Reduction in Data Volume

- Dramatic Decrease in MTTD/MTTM

- Dramatic increase in Operator Efficiency

Network Admission Control Integration



<u>Benefit:</u>

Ability to quickly locate and mitigate the source of an attack (MTTM is reduced)

Integration of Vulnerability Assessment

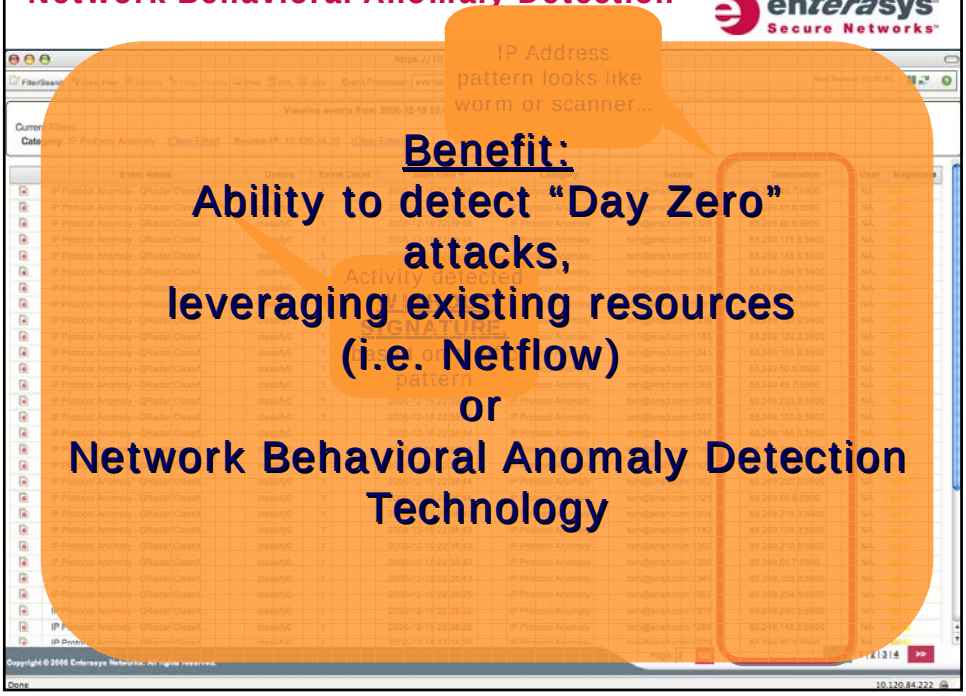
- Integrates vulnerability assessment technologies such as Nessus
  - Can integrate with others as well…
- Allows for data reduction/false positive reduction
  - If I attack an Apache server with an attack designed to compromise Microsoft IIS, then the attack is a false positive
- Reducing false positives reduces [illegible] security administrator
- Allows for [illegible] vulnerabilities

Benefit:

Constant monitoring for new vulnerabilities reduces risk, improves security position and infrastructure availability

Nessus Vulnerability Scanner

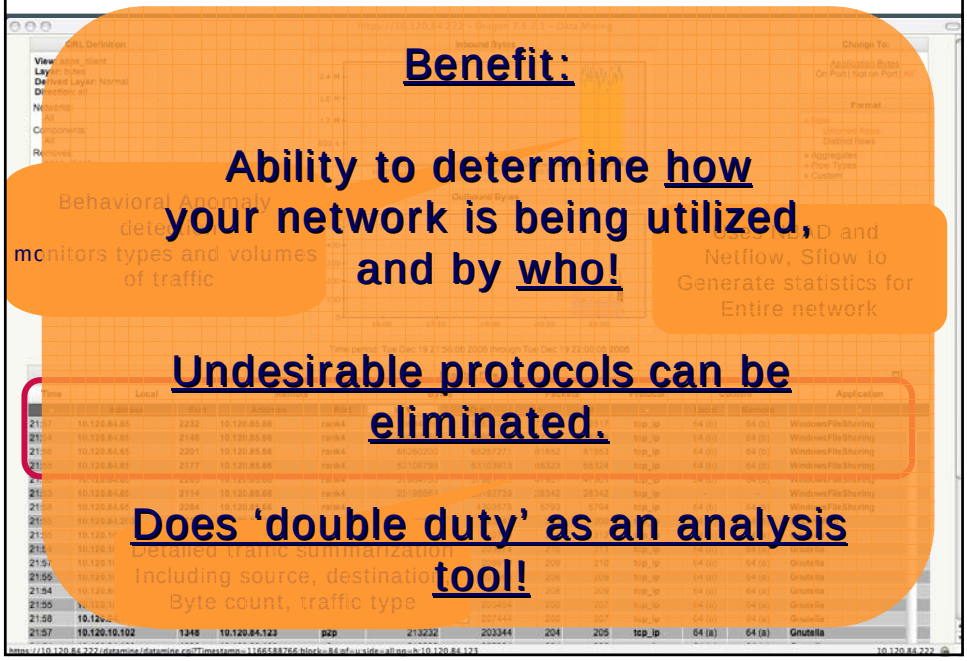
Network Behavioral Anomaly Detection



Benefit:

Ability to detect "Day Zero" attacks, leveraging existing resources (i.e. Netflow) or Network Behavioral Anomaly Detection Technology

Monitoring Network Utilization

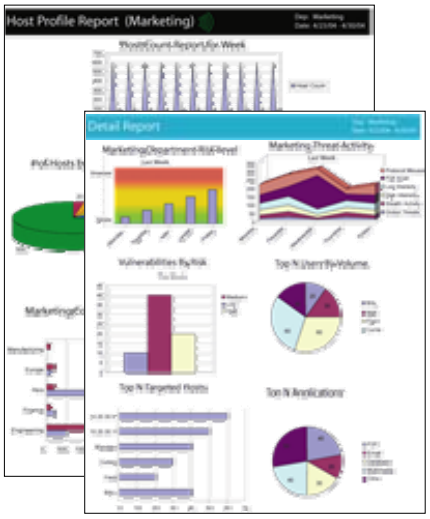


Leveraging Existing Infrastructure

- Traditional Network Devices:
  - Netflow
  - Syslog
  - Checkpoint OPSEC
  - SNMP Trap
- Existing IDS/IPS can be used…
  - Leverages existing investment in new ways
- Benefits:
  - More sensors available to improve analysis capabilities
  - Results in cost savings by extending existing investment

Reporting

- Reports must be available, **at the right level for the target audience!**
  - Executive Level Reports
    - High Level Enterprise wide or departmental Summary Reports
    - **Important because the customer needs to know he's getting what he's paying for!**
  - Operational Reports
    - Detailed Enterprise wide or departmental reports
  - Compliance Reports
    - Detailed for business obligations (SOX)
- The value of reporting is that it enhances your businesses compliance posture



Automated Log File Analysis

- Log files (or Windows events) analyzed in **real-time** by agent on end-system
- Log events "of concern" generate alerts to monitoring station
  - Examples: Security events, system events like overtemp or disk full, etc
- Vast majority of events in log file are irrelevant
- Monitoring personnel can take immediate action for critical events
- All events (mission critical and non-mission critical) are stored in centralized location for auditing and retention purposes
- **Benefits:**
  - **1)** Log files preserved in centralized location for archival
  - **2)** Events of interest are highlighted automatically, eliminating manual analysis and reducing staff workload
  - **3)** Latency in addressing critical issues reduced:
    - Manual analysis addresses only when logs are manually analyzed
    - Automatic analysis addresses issues as they happen