

# Intrusion Detection Systems



Gregory M. Tepe  
Director, Security Solutions

## ***What Is Intrusion Detection?***

- Detecting network break-ins
  - Detecting scans and probes
  - Detecting virus activity
  - Monitoring suspicious insider activity
  - Auditing logs from security devices
  - Correlating multiple security events
- Equates to Information Assurance !

## ***Why do Federal Agencies need IDS?***

- The threat is real
  - Insider (contractors, co-location facilities, malicious employees)
  - Outsider (external hackers, mistaken network security tests, foreign governments)
- When an attack occurs (and it will) companies will limit exposure, perform accurate damage assessment and have evidence for potential legal action
- Not a question of *whether* to install but *which* IDS to install

## ***Why do Federal Agencies need IDS?***

- Prevent problems by increasing the perceived risk of discovery, i.e. deterrence
- Detect problems that are not prevented by other security measures
  - uncorrected known vulnerabilities
  - open paths through firewalls
  - DMZ locations
- Detect preliminary attacks
  - probes
  - sweeps
  - scans

## ***Why do Federal Agencies need IDS?***

- Data Collection
  - monitor and document the threats
    - itemize and characterize internal and external threats
  - incident handling
  - recovery efforts
  - investigation

## ***Ideal Features of an IDS***

- \* High Speed Performance
  - \* Comprehensive
    - NIDS - Network-based IDS
    - HIDS - Host-based IDS
    - Management Station
    - Correlation Engine
  - \* Distributed Architecture
  - \* Scalable
- \* NIST Recommended

## ***Ideal Features of an IDS***

- \* Wide-ranging Detection of Attacks
  - \* Large Signature Database
  - \* System Anomaly Checks
  - Protocol Decoding Analysis
- \* Regular Signature Updates
- Open Signature Database

\* NIST Recommended

## ***Ideal Features of an IDS***

- \* Alarm Notifications
- \* Robust Forensics
  - Reports
  - Percentages
  - Long Term Trends

\* NIST Recommended

# **Dragon 6.0: Intrusion Detection System**

*Unparalleled, In-Depth Network, Host  
and Firewall Monitoring*



## ***Dragon 6.0 IDS Components***

### **Network Sensor**

- Network IDS
- 500Mbps throughput
- 2000+ detected attacks

### **Host Sensor**

- Host IDS
- Firewall/Router log monitor
- System/Web log monitor
- File monitoring
- OS Kernel logging

### **Dragon Server**

- Policy manager
- Event analysis
- Correlation Engine
- Customizable signatures
- Manage 500 Sensors
- Alarm Notification
- Distributed Architecture
- Scalable



## ***Sensor Architecture***

- 500MB Throughput
- Forensics for all events
- Largest signature database
- Open signature database
- System Anomaly Checks
- Protocol Decoding
- Command line and web analysis
- UNIX support – Solaris, BSD, Linux

# ***Dragon Management***

- Controls 500+ Dragon Sensors (NIDS and HIDS)
- Web management interface
- Distributable/Scalable
- Flexible event export log
- Event Correlation Tool
- Policy Manager
- Security Information Manager
  - Real Time Console (Live Data Analysis)
  - Forensics Console
  - Long Term Trending Tool
  - Performance Graphs
- Alarmtool (Perl, SNMP, SMTP and Syslog)

**ENTERASYS**  

---

**NETWORKS™**