



Managed Security Services

Intrusion Detection / Intrusion Prevention Service (IDS / IPS)

Yes, we have automated IPS that responds to predictable attacks within seconds. Yes, we have all the fancy charts and graphs and reports. But, with our managed services, human beings monitor your network. If something out of the ordinary happens, our Security Analysts are there in **real time** to **investigate** and **respond**.

infotex Security Analysts decipher the graphs and charts, review the data collected in your database, and create reports with varying levels of detail to share with your Incident Response Team. We're there 24x7x365, watching your network and **RESPONDING** to threats.



Our Intrusion Prevention Service can be in-line or utilize Dynamic ACL. For detection, we use thousands of signatures as well as protocol and anomaly analysis.

infotex also adds customized signatures to detect the issues and activities that you are most concerned about.

Our Decision Tree is a matrix listing all the predictable security incidents and your customized instructions as to the appropriate response. This includes a "first choice" to a "last resort" response. The result is that you will comply with Section 314.4(b)(3) of the FTC Standards for safeguarding customer information; final rule (16cfr, part 314). This ruling is a result of the GLBA that requires you to have a system in place for detecting, preventing and responding to attacks, intrusions or other system failures.

Just a Few of Our Managed Response IPS Basics –

- Human Response, Human Reporting
- Custom Designed Approach
- Time-testing Tuning Process
- Detailed Service Level Agreement (SLA)
- Proven Results!

Customized Service

Working one-on-one with you, **infotex** will develop layers of protection to fit well into your existing security management process, leveraging a suite of services.

Let **infotex** help your organization with your Managed Security Service needs!

Log Monitoring

infotex will monitor all logs fed to our sensors for critical and non-critical events and filter them down to actionable events. **infotex** will then respond in **real-time** to critical events per your customized business rules. Bandwidth is not tied up by massive log transfers to our Network Operations Center (NOC) . . . we only receive pertinent alerts and critical logs for analysis. There is no need for special encryption technologies just to monitor logs. A web interface will be made available for searching all events. Log storage lends itself to bullet-proof forensics analysis. On average, 2,600 logs per server per day are reduced to 2 actionable events.

Link Monitoring

Also called "ping monitoring," **infotex** will monitor all links documented by you on our managed services portal by connecting sensors to your network that ping critical links. These sensors will be configured and tuned to report all link outage events to our Network Operations Center. Security Analysts will monitor these events 24x7x365. In the event of an outage that is longer than 10 minutes, our Security Analysts will submit a ticket with your Internet Service Provider and notify appropriate client employees.

Port Scanning

infotex will scan a range of IP addresses on a periodic basis (weekly or monthly), reporting the ports that have changed since the last scan. Not only is this a great security tool, but it is an excellent change management tool as well.

System Performance Monitoring

infotex will monitor system load, disk space, and a number of other system attributes. **infotex** Security Analysts will alert appropriate personnel in the event of system load extremes, disk problems or errors, and any pre-defined event directives. **infotex** will also perform long term trending to be able to alert you when servers are being regularly pushed beyond load norms or are underutilized.