Controlled Response IPS

It's the Response that Counts!
We believe that information security goes beyond technology to include policies, procedures, and people. We don't sell a box that issues reports to shell-shocked IT Staff. The system doesn't page us so that we can hand off the incident to you. We go beyond that. We're there 24x7x365, watching your network and RESPONDING to threats.

Uniqueness
Our Intrusion Prevention Services are an ongoing infosec consulting engagement. It includes equipment, software, processes, procedures, boilerplates, and training. But, what makes our IPS unique is that it is all about the RESPONSE to an incident, rather than merely the reporting of the incident.

The Incident Response Policy (Fault Tree) is Key
When you engage us for the Controlled Response IPS, you open up a myriad of services that combines into the prerequisites required for us to provide true controlled responses to security incidents. These prerequisites range from deploying and training on communication tools such as our secure instant messenger and our IPS Portal (my.infotex.com) to developing response methodologies via our Incident Response Policy, or Fault Tree.

The Fault Tree is a matrix listing all the predictable security incidents and your instructions as to the appropriate response. This includes a "first choice" to a "last resort" response. Incidents are categorized by type, but you can be as granular as you want, so that our response to an incident meets your comfort level. 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 systems failures.

But Again . . . It's a Process
The tuning of your signatures does not stop after the two-month tuning period. Throughout the growth and evolution of your information system, we will continue to work with you to mitigate threats and ensure that your Intrusion Prevention System truly does provide adequate protection in your Security Management Process.

Controlled Response IPS Basics -

1) Custom Designed Signatures:
We use a group of open source and custom built applications to monitor your network and traffic. We place sensors on your network that report directly to our Network Operations Center (NOC). This data is monitored 24x7x365 by experienced Security Professionals. We use a set of over 2500 signatures to detect known issues, as well as protocol and anomaly analysis to find the things not yet known. We also add customized signatures to detect the issues and activities that you are most concerned about.

2) Time-Tested Prerequisites:
Prior to installing the system, we will walk your staff through a set of prerequisites that include reviewing existing risk assessments, signature tuning, documentation, portal training, fault tree design, offsite password management, and cost-mitigation training.

3) Service Level Agreement (SLA):
Unlike many IPS providers, we provide a detailed Service Level Agreement that specifies exactly what you can expect out of our service. There are several definitions that accompany our unique Service Level Agreement:

- IAM: Incidents allowed per month. Most of our programs allow 10 incidents per month.
- CRT: Complimentary Response Time. How much time is included with each incident to respond, contain, and advice.
- RRT: Required Response Time. This is the absolute guarantee we provide in the event of massive security events. We provide 1 hour, 4 hour, and 8 hour guarantees.

(Note: For quality control purposes, our average response time is kept at or below fifteen minutes.)