



Intrusion Detection / Prevention (IDS/IPS)



Human Response, Human Reporting!

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, a human

being is there in real time to investigate and respond according to your pre-defined instructions. Once per day, a human being deciphers the graphs and charts and sends you a report. On a monthly basis, a human being reviews the data collected in your database and sends you a report with varying levels of detail to share with your Incident Response Team. 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.

The Decision Tree is Key

When you engage us for the Managed 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. The Decision 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. 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.

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.

Customized Service

Working one-on-one with you, we will develop layers of protection to fit well into your existing security management process, leveraging a suite of services that includes port scanning, log monitoring, IPS, and IDS.

Just a Few of Our Managed Response IPS Basics -

1) Custom Designed Approach:

Our IPS can be in-line or we can work with existing routers or firewalls with Dynamic ACL updating to best deploy automated preventive services. For detection, we use thousands of signatures as well as protocol and anomaly analysis. We also add customized signatures to detect the issues and activities that you are most concerned about.

2) Human Response, Human Reporting:

Not all issues can be handled with automated response. Meanwhile, you are outsourcing your detection and response because you are NOT a security expert. We place sensors on your network that report directly to our Network Operations Center (NOC). This data is monitored 24x7x365 by experienced Information Security Professionals. These humans write daily reports directly to you about what has happened in the past 24 hours.

3) Time-Tested Tuning Process:

Installation includes a review of existing risk assessments, signature tuning, documentation review, portal training, decision tree design, offsite password management training and cost-mitigation training.

4) Service Level Agreement (SLA):

We provide a detailed Service Level Agreement that specifies exactly what you can expect out of our service.

5) The Proof:

We encourage you to talk to our existing clients about our customized approach to ensuring they are completely satisfied with our ability to help them understand the reports that we provide as well as help them sleep at night!