

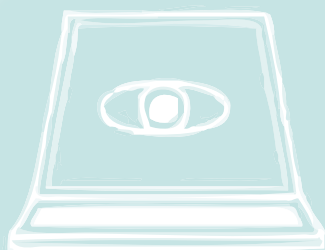
V S / I n s p e c t tm E x e c u t i v e S u m m a r y

Practical, cost-effective

Network Intrusion Detection

from Voyant Strategies

Executive
Summary



Overview

Businesses are relying on their data networks and internet connectivity more than ever. An outage, or even a slowdown, can cost thousands of dollars per hour in lost business and productivity. Very recently, a wave of malicious programs, known as 'worms', was released that have already caused severe disruptions in the business operations of companies that use technology to optimize their internal processes. While this phenomenon has existed for a long time now, its intensity is reaching a fever pitch, presenting a tremendous risk for any company connected to the Internet.

These malicious programs have been designed to get through or around the existing firewall and authentication technology that businesses have put into place, and to also be difficult to detect on networks whose entire security infrastructure consists of a firewall.

What is Intrusion Detection?

At its core, Intrusion Detection resembles a burglar alarm system, as it is capable of detecting a potential intrusion or policy violation, and sending alerts to a security engineer, providing guidance against any potential loss of integrity and confidentiality of the organization's valuable intellectual assets. It also can provide the forensic evidence necessary to take action against those responsible for an intrusion or network policy violation.

Firewalls and Secure Authentication devices are effective in protecting and preventing unauthorized access to the internal network, but they lack the capability to monitor the network itself, as they work only at the point of entry to the network. The majority of attacks, including worms and viruses, take place within the network, so these devices have a very limited ability to detect these malicious events.

Intrusion Detection – Definition by Analogy

Imagine you are in charge of Homeland Security, and have been put in charge of watching all traffic going through the highways in New Jersey. (This would be your network.)

By deploying a firewall-only strategy, you would simply have guards at the toll booths telling cars they could go, and stopping and searching trucks and buses. If a vehicle looks harmless and passes a few cursory examinations, it is allowed to pass.



Intrusion Detection will give you much more information such as what is in each car, what it will do when it gets to its destination, and whether the car is properly registered. This information allows for a much more complete picture to determine what threats exist, where they were targeting, and where they truly originated from.

What is the right way to perform Intrusion Detection?

Intrusion Detection is not something that can be simply bought and deployed, although there are many network hardware manufacturers that offer NIDS (Network Intrusion Detection) 'appliances'. In order to perform this function in an effective way, a seasoned security professional needs to constantly analyze the data that is generated by a well-configured Intrusion Detection infrastructure. VS/Inspect includes all the computing power required to accomplish this goal. It is the design, implementation, and maintenance of the NIDS infrastructure, as well as the ongoing analysis of the resulting data, that will mean the success or failure of an Intrusion Detection project.

VS/Inspect: On-Demand Intrusion Detection and Security Expertise

Voyant Strategies has been delivering best-in-breed Intrusion Detection processes for over 5 years. We augment your existing staff, allowing them to focus on their core business functions, while alerting them to any problems that are found on your network. Rather than trying to hunt down elusive problems, your IT staff is given specific information as to the root cause of problems, and given advice as to how to remedy those security issues.

We are also able to customize Intrusion Detection environments in order to satisfy policy and compliance requirements. For instance, we can watch for all cases of Social Security numbers traveling unencrypted through your firewall, or log all cases of P2P traffic, which violates most companies' network usage policies. Each client has different needs, and Voyant engineers provide both the guidance and expertise necessary to meet those needs. Our experienced staff also goes beyond mere alerting; we perform thoughtful ongoing analyses of the anomalous network traffic in your environment, not just the traffic that

would generate alarms. It is this human side of our offering that provides the greatest value, and it is also a primary reason other tool-based Intrusion Detection projects fail.

Our method of delivering this to you allows us to provide these services at a dramatic cost savings over attempting to provide this service to yourself.

Summary

Intrusion Detection is quickly becoming a necessity in most business environments today, as hackers and virus writers become more efficient at achieving their infiltration and damage through automatic, instant methods. It is imperative that you have the information at your disposal to make decisions and act quickly to stave off any possible damage and loss due to this nefarious activity.

Voyant's VS/Inspect is the most cost-effective and pragmatic way to achieve this level of network visibility.

VoyantStrategies
Envisioning the Future

Corporate Headquarters

45 Village Court
Hazlet, NJ 07730
(800) 463-7290

www.voyantinc.com

Copyright © 2004 Voyant Strategies, Inc. All rights reserved. Voyant Strategies, VS/Inspect, and the Voyant Strategies logo are registered trademarks of Voyant Strategies, Inc. or its affiliates in the U.S. and certain other countries. All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners.