

Managed Security Host-based Intrusion Detection (HIDS)

Overview

Cyber crime represents one of the most critical threats to businesses today. Attacks are so vast and complex that it has become impossible to detect every attack by hand. These attacks can cause downtime, or can create holes in system security for further breaches, and can eventually lead to financial losses, loss of credibility, or even regulatory compliance breaches.

Host-based Intrusion Detection System

Host-based Intrusion Detection Service (HIDS) is offered as a Managed Security Service within SAVVIS data centers and at customer premises. HIDS monitors customer servers and applications for malicious activity and other unauthorized use of host resources. The service includes ongoing monitoring of HIDS agents, security maintenance, alerting on intrusions and HIDS reports for customers. It includes software procurement, configuration, and installation, and is sold in conjunction with our Incident Response Service.

HIDS Service Elements

- Installation
- Configuration
- Monitoring
- HIDS Software Upgrades
- Maintenance and Support
- 24/7 Management by SAVVIS Managed Security Team

SAVVIS Managed Security Team

When an alert arrives, it is triaged by the SAVVIS Managed Security Team who will determine if your network and/or application host is under attack or has been breached. The Managed Security Team will then respond and implement the incident response plan created specifically for your business. SAVVIS Intrusion Detection Services are configured and installed per your specifications and are reviewed and updated on a semi-annual basis. Access to your alert reports for the previous 60 days are provided via a secure web-based interface. Working with SAVVIS to monitor and manage your intrusion detection systems helps you manage your IT

ADVANTAGES

- » Complements existing security solutions
- » Lower total cost of ownership – Outsourcing saves time and money in staffing and training
- » Online reporting - customer portal provides 24/7 access to service information.
- » Supports multiple platforms for interoperability
- » Capability to detect and respond to threats as they are occurring
- » Provides audit trail for event activity and forensic analysis
- » Improves visibility into attacks that travel down multiple connections

security costs by allowing your valuable staffing resources to focus on activities other than 24/7 alert monitoring.

For more information, contact a SAVVIS sales representative at 1 800 SAVVIS1.

