



Content Integrity Monitoring Service (CIMS)

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.

Content Integrity Monitoring Service (CIMS)

The SAVVIS Content Integrity Monitoring (CIMS) service provides notification and alerts when specified files residing on a host computer are changed. Alerts are then responded to 24/7 by SAVVIS' Managed Security team (if authorized by the customer).

Host-based software is provided that computes a cryptographic hash of the data content of a file and forwards that hash to an **integrity server** at a secure SAVVIS facility. The integrity server compares that hash with previously stored hash values for that same file — an integrity comparison. Any detected difference in hash values means that the directory or file has changed. CIMS is best used to monitor files and directories that tend to remain static.

CIMS Service Elements

- Monitoring of the directories and files residing on a host computer specified by the customer
- 40 hours per year of Incidence Response (IR) service in response to any detected security incidents
- Up to 120,000 integrity comparisons per day of system critical files residing on a host computer
- Expert consultation to determine which files or directories should be monitored
- Secure, authenticated, read-only access to integrity reports

SAVVIS Cyber Attack Team

CIMS is monitored 24/7 by SAVVIS' world class Managed Security Team for any potentially malicious or unauthorized activity. 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

ADVANTAGES

- » Complements existing security solutions by providing another line of defense at the file level
- » 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

Team will then notify you and implement the incident response and cyber forensics 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 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.

