

THREAT MANAGEMENT SERVICE

Overview

Our Threat Management Service provides an advanced view of critical IT assets, their vulnerabilities and the threats that are actively attempting to exploit those vulnerabilities. The service also provides a risk profile of these IT assets and can thus be an important component of your company's overall risk management strategy.

Threat Management Service Provides:

- Asset Valuation Tracking
- Correlation of Threats with Vulnerabilities*
- Internal Vulnerability Scanning
- Alerting*

**Requires separate purchase of SAVVIS' Managed NIDS Service*

Asset Valuation Tracking

First, your organization's infrastructure assets that are to be analyzed by the service must be identified and valued. The valuation is an aggregate figure, comprised of the potential value of the information, the cost of recovery, and an impact assessment. Five asset value categories are assigned: critical, high, medium, minor or low.

Once identified and valued, assets are entered into the Threat Management system. The system is updated on a predetermined basis or whenever significant changes are made to your infrastructure.

If your organization is not able to provide asset-value information, SAVVIS' Professional Services team can be engaged to perform a formal asset valuation.

Internal Vulnerability Scanning

After entry of assets into the system is completed, a scanner is installed in your infrastructure and an initial scan is performed to determine the vulnerability profile of your assets. The results of the initial scan are then exported to a correlation database. Regular scanning of both internal and external assets is scheduled to provide regular vulnerability updates to the correlation database.

Intrusion Detection

Threat identification is performed via SAVVIS' managed Network Intrusion Detection Service (NIDS), which must be purchased in conjunction with Threat Management under separate rates and terms. If your organization already has SAVVIS' managed NIDS service installed, it can be integrated to direct threat-incident information into an incident database.

Correlation of Threats with Vulnerabilities

When an incident is detected by SAVVIS' managed NIDS service, the threat is then correlated in real-time with vulnerability information to generate high-priority alerts that are detailed in reports that are available via our SAVVISStation Security Management Portal.

Alerting

All high-priority alerts are directed to the **SAVVIS 24x7 Security Operations Center (SOC)** where they are evaluated and subsequently escalated to the designated contact at your organization for resolution.

About SAVVIS

SAVVIS, Inc. (NASDAQ: SVVS) is a global leader in IT infrastructure services for business applications. With an IT services platform spanning North America, Europe, and Asia, SAVVIS is an industry leader in delivering secure, reliable, and scalable hosting, network, and application services. These solutions enable customers to focus on their core business while SAVVIS ensures the quality of their IT systems and operations. SAVVIS' strategic approach combines virtualization technology, a global network and multiple data centers, and automated management and provisioning systems.

KEY FEATURES

- Identifies attacks that pose the greatest threats to high-value assets, through real-time analysis and correlation of vulnerability and threat data
- Filters out most insignificant attacks, improving your ability to focus on fewer, more significant threats
- Leverages a market-leading third party scanning system for internal vulnerability scanning
- Robust portal, allows 24 x 7 access to the risk posture of IT assets and detailed reports

For more information about SAVVIS, visit www.savvis.net or call 1-800-SAVVIS-1.