

## SECURITY SERVICES

## Cisco®-Based Network Intrusion Detection Service



### Overview

Cyber crime represents one of the most critical threats to businesses today. Attacks are so widespread and complex that it has become impossible to detect them all manually. These attacks can cause downtime, or can create holes in system security for further breaches. They can eventually lead to financial losses, damage to brand credibility, or even jail time in the most extreme cases when executives are judged negligent.

### Cisco®-Based Network Intrusion Detection Service

Network Intrusion Detection Service (NIDS) is the core technology of a full set of Savvis security detection tools that give customers the ability to see security threats as they are en route to a host. Savvis provides NIDS services for installation in customer networks — both at Savvis data centers and on customer premises. Savvis configures, monitors, and maintains NIDS sensors to detect attacks against the target network. Detailed monitoring identifies malicious traffic, determines whether it has passed through the firewall, and traces the attacker's originating computer.

### Two NIDS Service Options are available:

- **Fully-Managed NIDS:** This is a complete solution that includes installation and management of Savvis-provided software and hardware. Customers who require services based on dedicated NIDS equipment, or who wish to get maximum value by utilizing Savvis' virtualized NIDS services, have a range of additional options.
- **NIDS Care:** This includes installation, configuration, and management of NIDS solutions that utilize customer-provided hardware and software.

### Savvis' Managed Security Team

NIDS is monitored on a 24/7 basis by Savvis' world-class Managed Security Team for potential malicious activity. When an alert is triggered, it is triaged by the Savvis Managed Security Team, which determines if your organization's network and/or application host is under attack or has been breached. The Managed Security Team will then notify you, and implement the incident response and cyber forensics plan that was created specifically for your business. Savvis' NIDS Services are configured and installed based on your requirements, and may be reviewed with you on a semi-annual basis. Access to your alert reports, signatures, and device activity for the previous 90 days is provided via a secure Web-based interface. (Additional information regarding NIDS reporting is available in the Appendix that follows).

### Key Features

- Round-the-clock access to Savvis' Incident Response Team
- NIDS appliances that are based on Cisco® technology
- Real-time intrusion monitoring and detection
- Aggregated multiple inbound connections to a single IDS device (an optional service, which is available separately)



Working with Savvis to monitor and manage your intrusion detection systems provides positive return on investment by augmenting your IT resources and relieving employees from 24/7 alarm monitoring and response requirements.

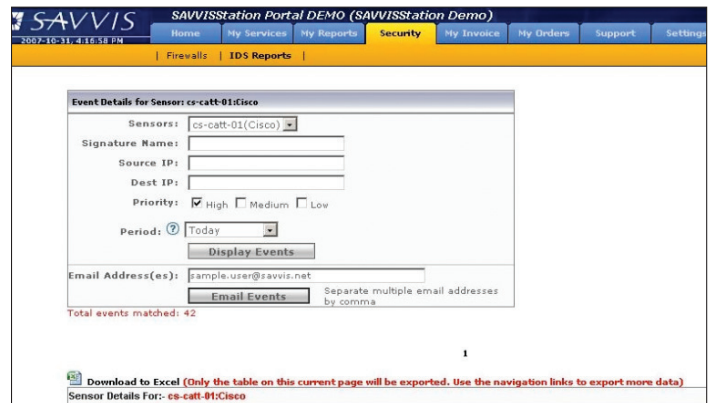
### Appendix: SavvisStation NIDS Reporting

Reporting for Savvis' Cisco®-Based NIDS Service is currently available through our SavvisStation Portal, which is a secure Web-based reporting interface. To enhance your organization's overall security, access to the portal is available solely to individuals who have previously been identified as "security contacts" by your organization. Portal support is available to customers on a 24/7 basis via a phone call or an e-mail to the Savvis Support Center.

Below are some demo screens that provide you with examples of the types of reports available on the portal. For a full explanation of SavvisStation portal functionality (including server performance reporting, network performance reporting and billing invoice options), please contact your Savvis Account Executive.

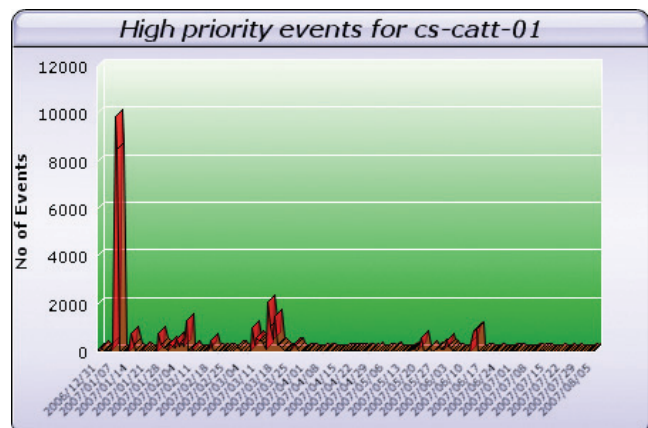
### SavvisStation Portal Main Security Page

Savvis has created a portal with functionality that allows your organization to search for specific signatures, Internet protocols (IPs), time periods, and priorities among all the alerts generated by your NIDS sensors or HIDS instances. You also have the capability to e-mail yourself entire reports, generate graphs, and download small sections of your data to Excel files.



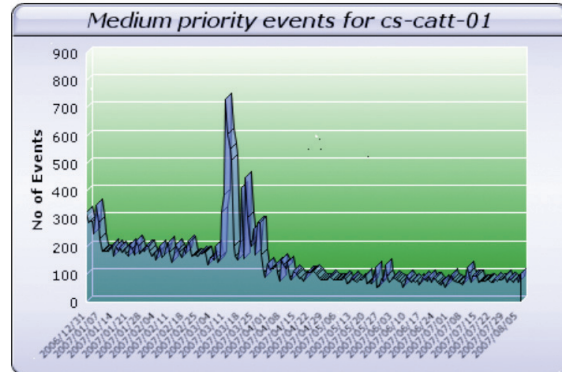
### Total Number of IDS Sensor High-Priority Events: Weekly View

This screen provides the total number of high-priority IDS Sensor events on a weekly basis. The graph utilizes demo data, and is not reflective of actual customer activity. If this graph depicted your organization's actual data, you would want to further research the activity that prompted a large spike in events during the first and second weeks of January 2007.



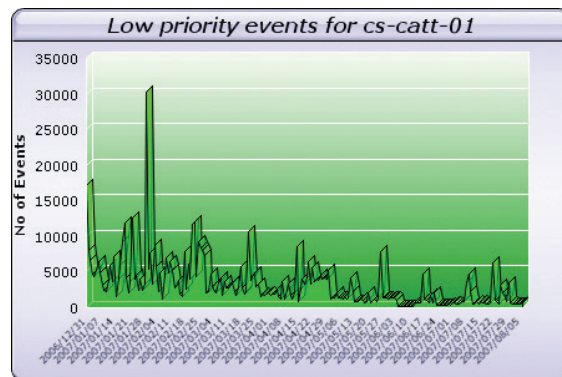
### Total Number of IDS Sensor Medium-Priority Events: Weekly View

This screen depicts the total number of medium-priority IDS Sensor events on a weekly basis. If this graph showed your organization's actual data, you would want to further research the activity that prompted a large spike in events during March and April 2007.



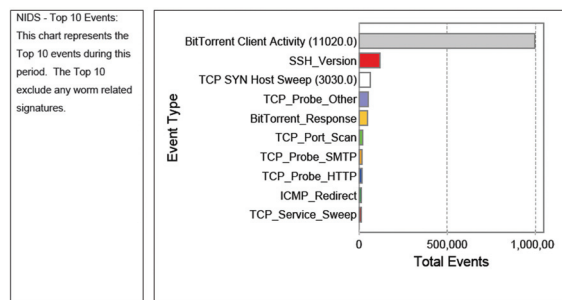
### Total Number of IDS Sensor Low-Priority Events: Weekly View

This screen provides the total number of low-priority IDS Sensor events on a weekly basis. If this graph depicted your organization's actual data, you would want to further research the activity that prompted a large spike in events in late January 2007.



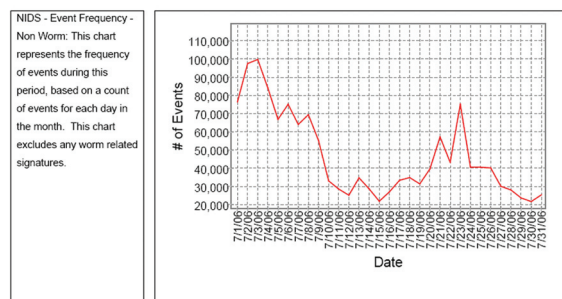
### Top 10 IDS Sensor Events for Time Period (excluding Worm-Related Signatures)

Based on the IDS Sensor activity that was presented in the first screen shot, this screen summarizes the Top 10 sensor events, including the number of times that the event occurred. You can see that the primary event affecting the demo sensor is BitTorrent Client Activity. Also note that worm-related signatures are not included in the summary that appears above.



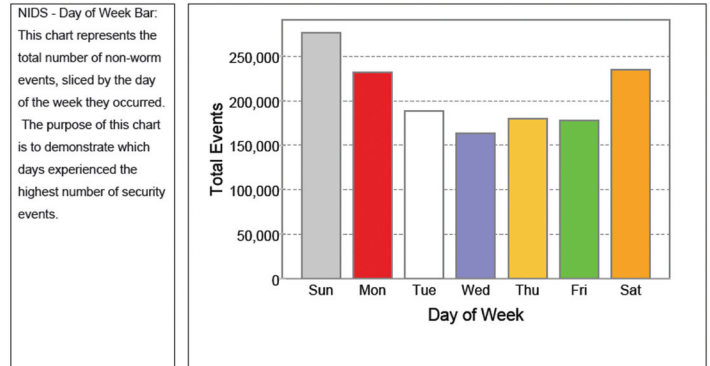
### Frequency of NIDS Event Activity (Daily View)

This screen summarizes NIDS events by date, allowing your organizational contact to track trends relating to potential intrusion. Based on the demo data here, it is clear that intrusion events seem to peak in the first and the third weeks of the month. Also, dates that show high levels of event activity — such as July 2 through 4, and July 22 through 25, in the example here — may be needed to be reviewed more closely by your security team. Note that worm-related signatures are excluded from the data that appears here.



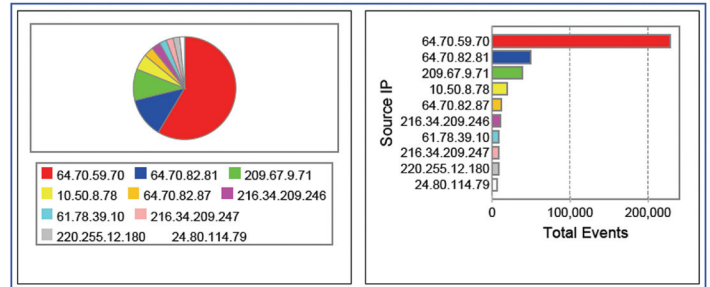
### NIDS “Day of the Week” Bar

This screen provides the total number of events by day of the week, allowing your organization to quickly determine which of the days resulted in the greatest number of non-worm-related IDS events. It is clear that weekends pose the most potential risk for IDS events when considering the historical demo event data that appear here.



### Summary of Source IP Addresses for IDS Events

The final screen-shot provides the source IP addresses for each of the IDS events. When evaluating the demo data in the chart, it is clear that the most persistent threat is coming from IP address: 64.70.59.70, which prompted more than 200,000 IDS events during the period. Events originating from that particular IP address comprised more than 50% of overall events for the period.



For additional information regarding Savvis’ Managed NIDS Services or the SavvisStation Portal, please contact your Savvis Account Executive.

### About Savvis

Savvis, Inc. (NASDAQ:SVVS) is an outsourcing provider of managed computing and network infrastructure for IT applications. By outsourcing to Savvis, enterprises can focus on their core business while Savvis ensures the quality of their IT infrastructure. Leading IT organizations around the world have selected Savvis to help them improve their service levels, reduce capital expense and deal with the rising costs of bandwidth, energy, real estate, staff and expertise. As a pioneer in utility computing, Savvis understands and harnesses the latest advances in technology like virtualization, cloud computing and support process automation.

For more information about Savvis, visit [www.savvis.net](http://www.savvis.net) or call **1.800.SAVVIS.1 (1.800.728.8471)**.

EMEA  
Savvis UK Limited  
Tel +44 (0)118 322 6000

ASIA PACIFIC  
Savvis Singapore  
Company Pte Ltd  
Tel +65 6768 8000

JAPAN  
Savvis Communications K.K.  
Tel +81.3.5214.0151