

SECURITY SERVICES

SNORT[®]-Based Network Intrusion Detection Service



Overview

Cyber crime represents one of the most critical threats to businesses today. These attacks can cause downtime, create holes in system security that result in data breaches, and lead to financial losses, brand credibility problems, or even jail time in those extreme cases where corporate executives are perceived as negligent. Attacks are so vast and complex that it has become impossible to detect and protect against them manually. Businesses need an automated solution that can help them identify when an attack is underway and take proactive measures before critical systems or data are damaged, stolen, or destroyed. Working with Savvis to monitor and manage your intrusion detection systems delivers a positive return on investment, by cost-effectively augmenting your IT resources with experienced personnel and relieving employees from routine 24/7 alarm management and monitoring duties.

SISD SNORT-Based Network Intrusion Detection Service

Savvis Integrated Security Device (SISD) network intrusion detection service (NIDS) is the core technology in a full set of security detection tools that offer customers the ability to view security threats en route to a host. We install, configure, monitor, and maintain the NIDS sensors for your organization in our data centers, where they detect potential attacks against your network. In addition, detailed monitoring enables identification of malicious traffic, determines whether the traffic has passed through your firewall, and even helps determine where an attacker's originating computer may be located.

Service Highlights:

Savvis provisions a SNORT-based NIDS device and works with your organization to implement the device. In addition to defining your organization's event escalation process, the SISD NIDS implementation includes:

- Ongoing signature event-tuning for newly-released signatures
- Management of your dedicated SISD SNORT-based intrusion detection device on a 24/7 basis
- Review of your intrusion detection system (IDS) events on a 24/7 basis
- Routine updates of your IDS sensor leveraging Sourcefire-based signatures

Key Features

- Alerts against unwanted internal or external network threats without degrading network performance
- Utilizes a NIDS infrastructure that leverages open source-based SNORT[®] technology
- Employs rigorous detection rules that are developed by Sourcefire's Vulnerability Response Team (VRT) and are rigorously-tested by Savvis prior to their implementation
- Provides round-the-clock access to Savvis' Incident Response team (Note: Incident Response Service is sold separately)



SNORT[®] is a registered trademark of Sourcefire, Inc.

Detection Rules Developed by Sourcefire's Vulnerability Research Team

To provide you with a high level of protection against potential threats, our service utilizes rules that are developed by the Sourcefire Vulnerability Research Team (VRT), a group of leading intrusion detection specialists. Savvis' use of these rules provides your organization with the following benefits:

- Sourcefire's rule-based protection methodology aims to provide protection before an exploit is released to the general public, thus reducing your potential "window of exposure."
- All rules are rigorously tested by Sourcefire and Savvis, with the goal of producing as few "false positive" results for your organization to review as possible.
- To maintain your network performance, rules are customized so that they are only triggered by certain communication states, network packet fields, and network message fields. The rules are further tested and verified by Sourcefire to confirm that they do not create performance issues when implemented.

Savvis' Security Operations Center Team

NIDS is monitored on a 24/7 basis by Savvis' experienced and credentialed Security Operations Center (SOC) team for any potential threat activity. When an alert arrives, it is triaged by the team, determining if your organization's network and/or application host is under attack, or possibly breached. The SOC Team will then notify you and implement the incident response and cyber-forensics plan that was created specifically for your organization. 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 our SavvisStation Portal.

Additional information regarding NIDS reporting is available in the Appendix that follows.

Appendix: SavvisStation NIDS Reporting

Reporting for Savvis' NIDS Services is currently available through our SavvisStation Portal, 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.

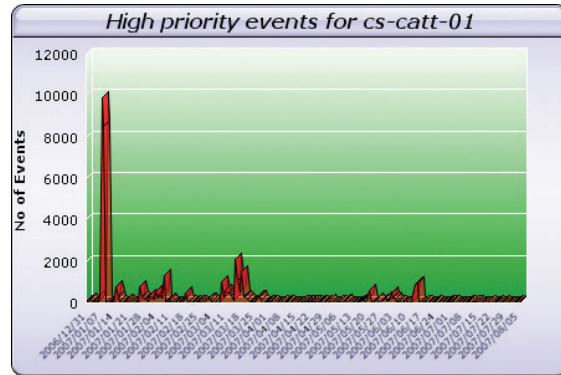
The portal provides functionality that allows your organization to search for specific signatures, Internet protocols (IPs), time periods, and priorities among all the alerts generated by your NIDS sensors or host-based intrusion detection system (HIDS) instances. You also have the capability to e-mail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

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.

The following screen depictions are for illustrative purposes only.

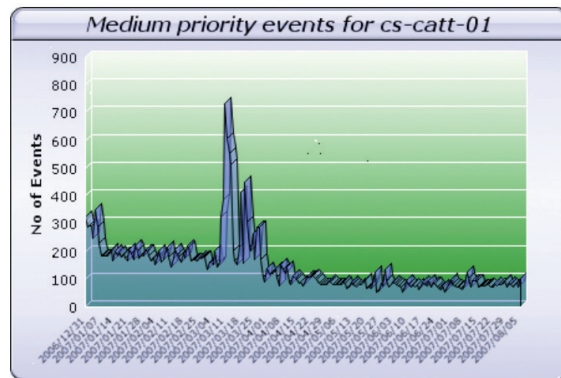
Total Number of IDS Sensor High-Priority Events: Weekly View

This screen shows the total number of high-priority IDS Sensor events on a weekly basis over an eight-month period. If this graph depicted your organization's actual network activity, you would want to further research what prompted a large spike in events during the first and second weeks of January 2007.



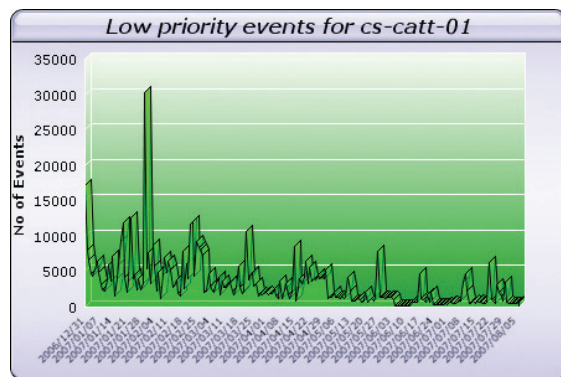
Total Number of IDS Sensor Medium-Priority Events: Weekly View

This screen provides the total number of medium-priority IDS Sensor events on a weekly basis over the same eight-month period. If this graph depicted your organization's actual activity, you would want to further research what prompted a large spike in events during March and April 2007.



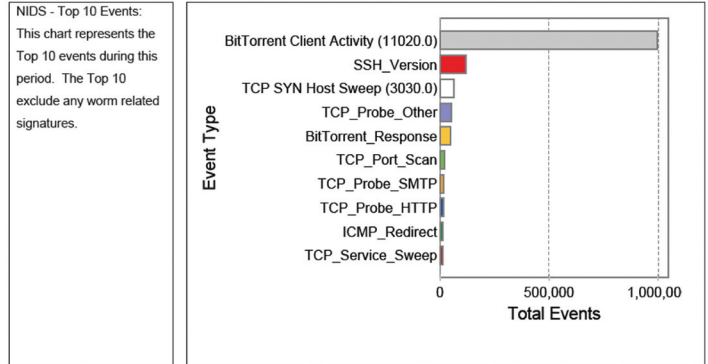
Total Number of IDS Sensor Low-Priority Events: Weekly View

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



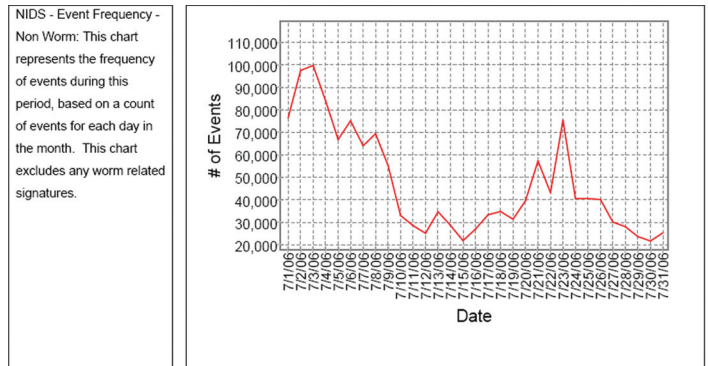
Top 10 IDS Sensor Events for Time Period (excluding Worm-Related Signatures)

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, it should be noted that Worm-related signatures are not included in the summary that appears to the right.



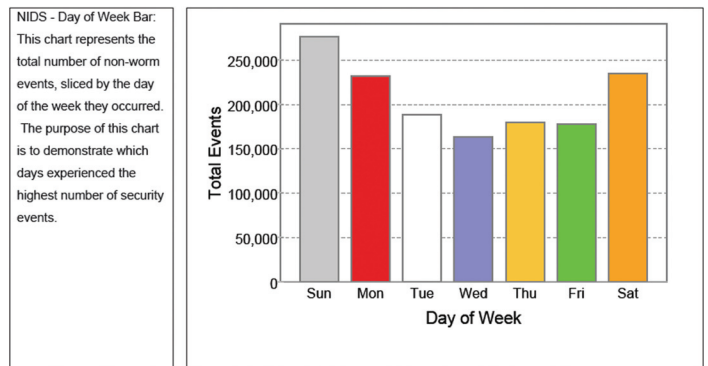
Frequency of NIDS Event Activity (Daily View)

This screen summarizes NIDS events by date, allowing your organizational contact to track trends relating to potential intrusion. Based on the demo data above, 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), may be needed to be reviewed more closely by your security team. (Worm-related signatures are excluded from the data that appears to the right).



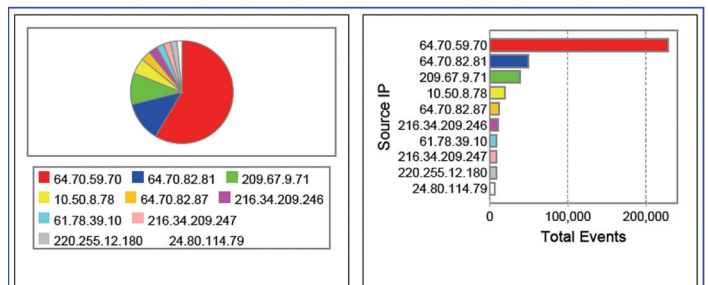
NIDS "Day of the Week" Bar

This screen provides the total number of events by the 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 appears to the right.



Summary of Source IP Addresses for IDS Events

This final screen shot provides the source IP addresses for each of the IDS events. When evaluating the demo data in the chart to the right, 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' SNORT-based NIDS Service or the SavvisStation Portal, please contact your Savvis Account Executive.

About SNORT®

In 1998, Martin Roesch wrote an open source technology called SNORT®, which he termed a "lightweight" intrusion detection technology in comparison to commercially available systems. Today that moniker doesn't even begin to describe the capabilities SNORT® brings to the table as the most widely deployed intrusion prevention technology worldwide. Over the years SNORT® has evolved into a mature, feature rich technology that has become the de facto standard in intrusion detection and prevention. Recent advances in both the rules language and detection capabilities offer the most flexible and accurate threat detection available, making SNORT® the "heavyweight" champion of intrusion prevention. For additional information about SNORT®, please consult www.snort.org.

Savvis is a Certified SNORT® Integrator. Please refer to the following link for details: <http://www.snort.org/community/integrators.html>.

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 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