



## INTELLIGENT EVENT MODULE BASICS

The Sourcefire Snort 2.6.0 Intelligent Event Module (IEM) enables you to automate real-time monitoring of your network intrusion prevention systems using Snort 2.6.0 and capture the critical information you need for effective enterprise security management.

The Sourcefire Snort 2.6.0 IEM provides ConsoleWorks® with a watch-list of text messages, including intrusion alerts, traffic analyses, and vulnerability detections, produced by the Snort ruleset 2006-06-27. ConsoleWorks watches for these messages, called Events, in the data streams of your managed firewalls and intrusion prevention systems.

**Note:** This IEM includes Events produced by the Snort Preprocessor (SPP) rules.

### Events

When ConsoleWorks detects an Event, it alerts you to the Event as it is happening, records the circumstances surrounding the Event, and automatically performs the default or customer-configured responses associated with that Event.

### Scans

IEMs come with Events pre-arranged in logical groupings, called Scans™. Working with a Scan—or a combination of Scans—instead of hundreds of individual Events simplifies managing Events across your enterprise.

## SOURCEFIRE SNORT 2.6.0 IEM AT A GLANCE

Events:	7738
Scans:	1 Master 3 Event Severity
Filename:	<code>cw_iem-sourcefire_ snort-0004.bin</code>
License Required:	<code>CONWRKS-DB-SNORT.lic</code>
Connector Required:	Syslog

## USING THE SOURCEFIRE SNORT 2.6.0 IEM

To use this IEM, complete the following tasks:

1. Download the IEM from the TDi web site.
2. Import the IEM into ConsoleWorks.
3. Associate the Scans from the IEM with the firewalls you want to manage.

### To Download the IEM

1. Install the license for the Sourcefire Snort 2.6.0 IEM. To obtain this license, contact your TDi Solutions Team Manager ([sales@tditx.com](mailto:sales@tditx.com)).
2. Move to the TDi web site ([www.tditx.com/support\\_iemdownloads.asp](http://www.tditx.com/support_iemdownloads.asp)).
3. On the Product Downloads page, locate and click **Sourcefire Snort 2.6.0**.
4. In the Connect to support2.tditx.com dialog box, enter your User name and Password, and click **OK**. To obtain a User name and Password, contact TDi Support ([support@tditx.com](mailto:support@tditx.com)).
5. Save the file (`cw_iem-sourcefire_snort-0004.bin`) to a directory accessible from your client workstation.

### To Import the IEM

1. On the ConsoleWorks main menu, click **Admin > Database > Import IEM**.
2. On the Import IEM page, click **Browse**.
3. On the Choose file dialog box, locate and double-click `cw_iem-sourcefire_snort-0004.bin`.
4. On the Import IEM page, click **Import IEM**, and wait for the **IEM import completed** message to appear on the page before associating the IEM's Scans.

### To Associate the Scans

Associate the Scans with the Snort 2.6.0 firewalls/intrusion prevention systems you want ConsoleWorks to monitor. When you associate Scans with a system, you are specifying that ConsoleWorks scan the data streams of that system for the Events contained in the Scans.



### Example: To associate SNORT\_CRITICAL Scan

1. On the ConsoleWorks main menu, click **Manage > Scans > Show Scans**.
2. On the Show Scans page, in the Scans column, click **SNORT\_CRITICAL**.
3. On the Scan: SNORT\_CRITICAL page, in the Unassociated Consoles column, select the check boxes next to the names of the managed firewalls you want to associate with the Scan.
4. Click **Update Scan**.

For detailed instructions on associating Scans, please refer to the ConsoleWorks user's guide.

## SCANS AVAILABLE IN THE SOURCEFIRE SNORT 2.6.0 IEM

The Sourcefire Snort 2.6.0 IEM contains a Master Scan and three Event Severity Scans.

### Master Scan

The Master Scan, **SNORT**, is the top-level Scan. It references all the other Scans in the IEM. When you associate the Master Scan with an intrusion prevention system, you are specifying that ConsoleWorks scan the data streams of that system for any of the IEM's 7,738 Events.

### Event Severity Scans

The Sourcefire Snort 2.6.0 IEM contains three Event Severity Scans. Use one or more of these Scans to monitor Snort 2.6.0 for Events based on their Severity level.

The IEM provides the following Event Severity Scans:

- SNORT\_CRITICAL 3083 Events
- SNORT\_MAJOR 1407 Events
- SNORT\_MINOR 3248 Events

## SAMPLE SOURCEFIRE SNORT 2.6.0 IEM EVENT

The Sourcefire Snort 2.6.0 IEM provides you with names, message texts, Severity ratings, explanations, rule information, attack scenarios, recommended responses, and other information about Events produced by Snort 2.6.0.

The following section displays a sample of the information you receive for each Event in the Sourcefire Snort 2.6.0 IEM.

### Sample Event 1

**Name:** SNORT\_0215  
**Message:** :215:  
**Severity:** CRITICAL  
**Explanation:** BACKDOOR MISC Linux rootkit attempt. This Event is generated when an attacker attempts to connect to a Telnet server using the phrase "d13hh[ ".  
**Rule Header:** alert tcp \$EXTERNAL\_NET any -> \$TELNET\_SERVERS 23  
**Rule File:** backdoor.rules (line 147)  
**Content:** "d12hh[ "  
**Impact:** Possible theft of data and control of the targeted machine leading to a compromise of all resources the machine is connected to.

**Detailed Information:** This Trojan affects Linux operating systems: Due to the nature of this Trojan it is unlikely that the attacker's client IP address has been spoofed.

**Attack Scenarios:** This Trojan may be delivered to the target in a number of ways. This Event is indicative of an existing infection being activated. Initial compromise may be due to the exploitation of another vulnerability and the attacker is leaving another way into the machine for further use.

**Corrective Action:** Disallow Telnet access from external sources. Use SSH as opposed to Telnet for access from external locations Delete the Trojan and kill any associated processes.

© 2007 TECSys Development, Inc. The information in this document is provided by TECSys Development, Inc. as-is without warranty of any kind and is subject to change without notice. The warranties for TECSys Development, Inc. solutions are set forth in the limited warranty statements accompanying such solutions. Nothing herein shall be construed as constituting an additional warranty. All products or company names mentioned in this document are trademarks or registered trademarks of their respective owners. Portions of the technology within the ConsoleWorks server are protected under US Patent number 6,505,245. ConsoleWorks is a registered trademark of TECSys Development, Inc.