IBM OpenSignatures

OpenSignatures
User Guidelines

Publication Date: December, 2011

Chapter 1. Overview

Use the OpenSignatures feature to write customized, pattern-matching signatures to detect threats that are not preemtively identified by IBM® Security Network Intrusion Prevention System (IPS) products.

Benefits

Use the OpenSignatures feature to set up the following protections:

- Audit signatures for Layer 6 and 7 applications that are specific to your environment
- Signatures that name a specific attack variant for customized reporting purposes

Restrictions

The OpenSignatures feature is integrated into the IBM Protocol Analysis Module (PAM) as a rule interpreter, and it relies on PAM and the IBM security product you have installed on your network to work.

Important: IBM Customer Support is not available to help you write or troubleshoot custom rules for your environment. If you require assistance to create custom signatures, please contact IBM Professional Services.

Supported agents

You can use the OpenSignatures feature with the following agents:

- IBM Security Network Intrusion Prevention System (IPS), versions 1.2 and later
- IBM Proventia® Desktop
- IBM RealSecure Network Sensor
- IBM Proventia Virtual Server Protection (VSP)

Important: These guidelines assume that you are managing these agents through the SiteProtector System Console, and that you are not manually editing configuration files.

The OpenSignatures Author's Guide

Use this document in conjunction with the *OpenSignatures Author's Guide* to manage the OpenSignatures feature. The Author's Guide explains general syntax for OpenSignatures. It also describes options for rules, options for modifiers, flow tracking, and PCRE and post-PCRE keyword modifiers.

Considerations

The OpenSignatures feature is very flexible, and you can use it to create rules for many purposes. However, this flexibility also makes it possible for you to create rules that you did not intend to create. This topic explains the risks of using OpenSignatures rules.

Use care when you create a rule

Poorly written rules or signatures can impact sensor performance or have other consequences. Using your own custom signatures include, but are not limited to, the following risks:

- Causing unacceptable appliance performance
- Causing the agent to go into an infinite loop

- Blocking all network traffic to a specific segment (inline mode, with or without a bypass)
- Having to reinstall the appliance's factory image to return it to a "good" state

Prevention or detection

For Proventia Desktop, Proventia Virtual Server Protection (VSP), and RealSecure Network Sensor, OpenSignatures rules can detect events, but cannot block them.

For Security Network IPS, OpenSignatures rules can both detect and block events.

Support limitations

IBM Customer Support is not available to help you write or troubleshoot custom rules for your environment. If you need assistance with creating custom signatures, please contact IBM Professional Services.

A poorly written signature can cause a performance issue that may not appear to be related to the signature. IBM Customer Support may ask you to disable the OpenSignatures feature, and then reproduce the performance issue, before troubleshooting the issue.

Chapter 2. Enabling the OpenSignatures Feature

The parser that interprets your signature rules is disabled by default. To enable the parser, you must add a custom tuning parameter to a SiteProtector System policy, and then apply that policy to your sensor.

Enabling OpenSignatures for Security Network IPS GX6000 series appliances

Procedure

1. On the Global Tuning Parameter page, click **Add**.
2. Change the following options as necessary:

Option	Description
Name	`engine.OpenSignatures.enabled`
Value	`true`

Enabling OpenSignatures for non-GX6000 series Security Network IPS appliances

Procedure

1. On the Global Tuning Parameter page, click **Add**.
2. Change the following options as necessary:

Option	Description
Name	`pam.trons.enabled`
Value	`true`

Enabling OpenSignatures for Proventia Desktop versions 8.0 and 9.0

Procedure

1. In the SiteProtector System, go to the Proventia Desktop policy editor.
2. In Network Protection, select **Default Settings** > **Intrusion Prevention Settings** > **Custom IPS parameters**.
3. Click **Add**.
4. Change the following options as necessary:

Option	Description
Name	`pam.trons.enabled`
Value	`true`

Enabling OpenSignatures for Proventia Desktop version 10.0

Procedure

1. In the SiteProtector System, go to the Proventia Desktop policy editor.
2. In the **Security Events Default Settings**, go into **Advanced Configuration**.

3. Click **Add**.
4. Change the following options as necessary:

Option	Description
Name	`pam.trons.enabled`
Value	`true`

Enabling OpenSignatures for Network Sensor

Procedure

1. In the SiteProtector System, select the **Sensor** tab.
2. Right-click your Network Sensor, and then select **Edit Properties**.
3. Select the **Advanced Parameters** tab.
4. Click **Add**.
5. Change the following options as necessary:

Option	Description
Name	`pam.trons.enabled`
Type	Boolean
Value	`true`
Description	Type a description for the rule

Enabling OpenSignatures for Network Sensor by policy

Procedure

1. In the SiteProtector System, select the **Sensor** tab.
2. Select the Network Sensors for which you want to apply the policy, and then select **Apply Policy**.
3. Select the **Custom** policy.
4. Select the **X-Press Update** tab within the policy editor.
5. Select the group within the XPU.
6. Click the **Tuning** button.
7. Click **Add**.
8. Change the following options as necessary:

Option	Description
Name	`pam.trons.enabled`
Type	Boolean
Value	`true`
Description	Type a description for the rule

Enabling OpenSignatures for Virtual Server Protection for VMware

Procedure

1. In the Navigation pane, click the **Site Group** and then open the Policy view for Proventia Server for VMware.
2. Right-click **Security Events**, and then click **Open**.

3. In the **OpenSignaturess** tab, click the **Add** icon or highlight the rule you want to edit, and then click the **Edit** icon.

   Tip: You can edit some properties directly by double-clicking the item you want to configure.
4. Select the **Enabled** check box.
5. Change the following options as necessary:

Option	Description
Description	Describes the purpose of this signature
Rule string	Specifies the text string that tells the agent when an event is triggered

Chapter 3. Adding an OpenSignatures Rule

The procedure for adding a custom rule varies from product to product. This section contains the information you need in order to add OpenSignatures rules to a specific product. This procedure is not applicable to Proventia Virtual Server Protection (VSP).

Adding a rule for IBM Security Network IPS appliances

Procedure

1. In Local Management Interface , go to the OpenSignatures section.
2. Change the following options as necessary:

Option	Description
Enable	Select the check box to enable the rule.
Comments	Type a description for the rule.
Rule String	Type the text string that tells the appliance when an event is triggered.
Event Throttling	Type an interval value in seconds. At most, one event that matches an attack is reported during the interval you specify. A value of 0 (zero) disables event throttling.

Adding a rule for Proventia Desktop 8.0 or 9.0

Procedure

1. In the SiteProtector System, go to the Proventia Desktop policy editor.
2. In Network Protection, select **Default Settings** > **Intrusion Prevention Settings** > **Custom IPS parameters**.
3. Click **Add**.
4. Change the following options as necessary:

Option	Description

Name	pam.trons.rules.*n*
	
	where *n* is an integer value. This value must be unique if you are entering multiple OpenSignatures rules.
	Example:
	
	`pam.trons.rules.1, pam.trons.rules.2,`
	
	`pam.trons.rules.100`

Value	Type the rule. **Example:** `alert tcp 192.168.1.0/24 any . .192.168.1.10 80(msg:"This rule triggered on html"; content:"html"; nocase; sid:10;)`

Adding a rule for Proventia Desktop 10.0

Procedure

1. In the SiteProtector System, go to the Proventia Desktop 10.0 policy editor.
2. In the Security Events Default settings, go to Advanced Configuration.
3. Click **Add**.
4. Change the following options as necessary:

Option	Description

Name	pam.trons.rules.*n*
	
	where *n* is an integer value. This value must be unique if you are entering multiple OpenSignatures rules.
	Example:
	
	`pam.trons.rules.1, pam.trons.rules.2,`
	
	`pam.trons.rules.100`

Value	Type the rule. **Example:** `alert tcp 192.168.1.0/24 any . .192.168.1.10 80(msg:"This rule triggered on html"; content:"html"; nocase; sid:10;)`

Adding a rule for Network Sensor

Procedure

1. In the SiteProtector System, select the **Sensor** tab.
2. Right-click the Network Sensor, and then select **Edit Properties**.
3. Select the **Advanced Parameters** tab.
4. Click **Add**.
5. Change the following options as necessary:

Option	Description

Name	pam.trons.rules.*n*
	
	where *n* is an integer value. This value must be unique if you are entering multiple OpenSignatures rules.
	Example:
	
	`pam.trons.rules.1, pam.trons.rules.2,`
	
	`pam.trons.rules.100`
	Note: You can enter more than one rule at a time. You must encode multiple rules in BASE64 format, and then enter the rules as a single line of text. SiteProtector allows a maximum of 10,000 bytes of text in a field, which limits the number of rules that you can enter in each block.

Option	Description
Type	Select **String**.
Value	Type the rule. **Example:** `alert tcp 192.168.1.0/24 any . .192.168.1.10 80(msg:"This rule triggered on html"; content:"html"; nocase; sid:10;)`
Description	Type a description for the rule.

Adding a rule for multiple Network Sensor installations

Procedure

1. In the SiteProtector System, click the **Sensor** tab.
2. Select the sensors, and then select **Apply Policy**.
3. Select the **Custom** policy.
4. Select the **X-Press Update** tab within the policy editor.
5. Select the group within the XPU.
6. Click the **Tuning** button.
7. Click **Add**.
8. Change the following options as necessary:

Option	Description

Name	pam.trons.rules.*n*
	
	where *n* is an integer value. This value must be unique if you are entering multiple OpenSignatures rules.
	Example:
	
	`pam.trons.rules.1, pam.trons.rules.2,`
	
	`pam.trons.rules.100`
	Note: You can enter more than one rule at a time. You must encode multiple rules in BASE64 format, and then enter the rules as a single line of text. SiteProtector allows a maximum of 10,000 bytes of text in a field, which limits the number of rules that you can enter in each block.

Type	Select **String**.
Value	Type the rule. **Example:** `alert tcp 192.168.1.0/24 any . .192.168.1.10 80(msg:"This rule triggered on html"; content:"html"; nocase; sid:10;)`
Description	Type a description for the rule.

Chapter 4. Setting Responses for OpenSignatures Rules

You can use the Central Responses feature in the SiteProtector System to set up responses for OpenSignatures rules for Network IPS and on a network sensor. These responses include SNMP, SMTP, Log Evidence, and User Specified Events.

For detailed information about using the Central Responses feature, see the *IBM Security SiteProtector System Configuration Guide*.

Note: If you format an OpenSignatures rule incorrectly, the SiteProtector System displays a PAM configuration error in the Sensor Analysis view.

Setting up responses on a Security Network IPS appliance

You must add some global tuning parameters to the Security Network IPS appliance before you can block an event with an OpenSignatures rule.

Example:

```
alert tcp any any -> any any (msg:"Yahoo accessed"; content:"yahoo"; nocase; sid:5000;)
```

In this example, 6005000 is the Issue ID that you would see in the alert message when the rule is triggered. Use this Issue ID in Global Tuning Parameters when you set the response.

To set the block response for this sample rule, you would set the following values in the Global Tuning Parameters section of Proventia Manager:

- `np.vs.0.issue.6005000=on`
- `np.vs.0.issue.6005000.response=drop-packet,reset-intruder,resetvictim`

Use this method to set the block response for any OpenSignatures rule. Always use your own rule ID instead of the ID (6005000) used in the example.

Setting up responses on a network sensor

About this task

You can assign responses to the OpenSignatures rule by adding a response parameter to the sensor properties or in the policy that uses the issue.issue_ID.response parameter. Use the Issue ID that is created from the ID assigned in the rule.

Procedure

1. Open the sensor properties or the policy you want to modify.
2. Change the following option as necessary:

Option	Description
Name	Type the following value: `issue.`*`issue_ID`*`.response`where *issue_ID* is the Issue ID the system created (by adding 6,000,000 to the one to four digit identifier you selected).

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Office 4360
One Rogers Street
Cambridge, MA 02142
U.S.A

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Trademarks

IBM, the IBM logo, and ibm.com, and Lotus® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Printed in USA