ThreatFactor.com

QUICK START GUIDE

Getting Started

This guide will walk you through how to install and begin using ThreatFactor NSIA. Preparing NSIA is easy and should not take more a few minutes.

Requirements

NSIA requires the free Sun Java Runtime (JRE) version 6 or higher. Note that the installers will attempt to determine if you have Java installed already. By default, NSIA listens on port 8080; therefore, you may need to open this port on your firewall to access NSIA remotely.

Download and Installation

NSIA can be downloaded for free from ThreatFactor.com. You can install it either via the Windows installer, Debian package (for Ubuntu) or with the zip archive.

Installing on Windows

For Windows, use the installer (ThreatFactor NSIA Setup.exe) to install NSIA. The installer includes a Windows service that can be started with services.msc.

Installing on Ubuntu (with the Debian Package)

For Ubuntu, use the Debian package to install NSIA. You can install the package with Synaptic or from the command-line with the following (assumes that the name of the package is nsia-0.9.3.deb:

```
sudo dpkg -i nsia-0.9.3.deb
```

Once installed, NSIA will be running on port 8080 (http://127.0.0.1:8080).

Installing on Other Platforms (using the Zip Archive)

You can also NSIA by unzipping the files from the zip archive. To install, just unzip to a directory. Next, run either install.bat (on Windows) or install.sh (on Unix) to complete the installation.

Getting Definitions

You can get a license for free by registering at ThreatFactor.com. Registering allows you to obtain a license key that can be entered into NSIA; this allows NSIA to download new definitions automatically.

If you don't want to register, just download the definitions and install them manually. Definitions can be downloaded from ThreatFactor.com and installed by importing them on the definitions management page in NSIA (upload the file into NSIA by going to Main Dashboard → View Definitions → Import Definitions).

Need Help or Information?

See the links below for additional information:

- Product information
- User guide / wiki
- Downloads
- View or report a bug
- Request support or new features
- Download source code

For more information, visit ThreatFactor.com

NSIA is an open source project

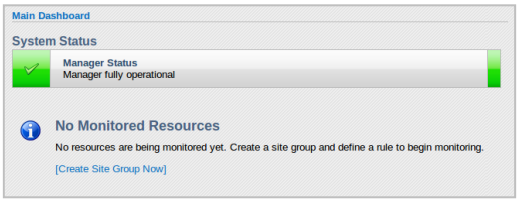
sourceforge

Begin Monitoring

To begin monitoring a website, you'll need to create the appropriate rules. See below for directions to get started.

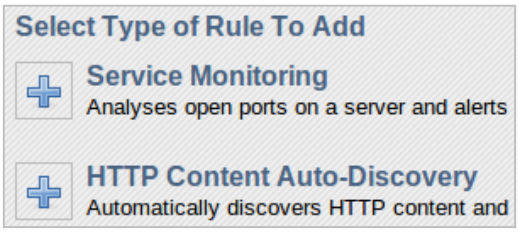
Step 1: Create a Site-Group

To start monitoring a site, create a new site-group. A site-group is simply a collection of monitoring rules. You can start by creating one with the name of the website you want to monitor.



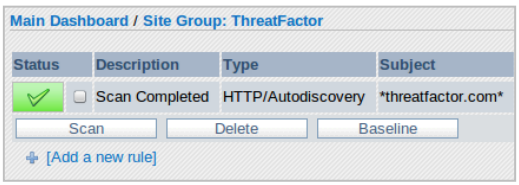
Step 2: Create a Rule

Next, create a new rule. To monitor the content of a website, create a new "HTTP Content Auto-Discovery" in the site-group you previously created. Add at least one start address and set the parameters necessary to begin scanning.



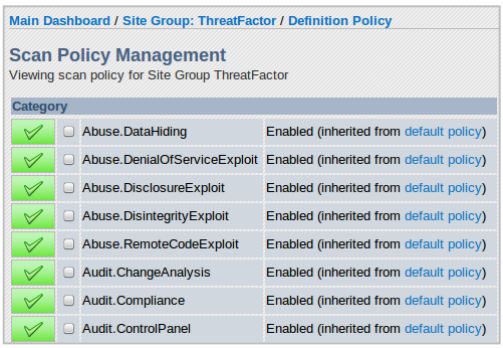
Step 3: Baseline the Rule

Once the rule is created, select the rule and press scan. Once it is scanned, you can view the results. NSIA will likely find some things that are not issues you care about. You can baseline the rule in order to automatically filter out the current set of findings. To baseline the rule, select the rule and press baseline.



Step 4: Customize the Scan Policy

Over time, you may find that you need to disable some definitions that may not be appropriate for a particular site. For example, you may want to disable the "Audit.ChangeAnalysis.Content_Changed" definition if your site changes often. To customize the scan policy, open the site-group you want to customize and select "Edit Scan Policy". Next, select the definition categories you would like to enable or disable and apply the changes.



Step 5: Start Scheduled Scans

By default NSIA does not enable the scanner to perform the scheduled scans. To start it, just click "Start Scanner" from the main dashboard. If you want the scanner to automatically start every time NSIA is restarted then enable it on the configuration page. To do this, go to Main Dashboard ➔ System Configuration and set "Scanner Default State" to enabled.