Syspeace Detector Providers for System Administrators

Detectors explained

Syspeace continuously protects your server by blocking attackers when they fail to login. Syspeace does this by applying rules to find patterns in login attempts, looks for matches for these patterns and turns them into blocks. But how does Syspeace find out about the login attempts? By using **detectors**.

Syspeace contains a number of detectors built-in and each detector continuously looks for records about login attempts. For example, there's a Windows login detector, which looks for Windows account logon audit events. The detector takes the data Syspeace needs and passes it into the Syspeace engine. When a detector transforms a login attempt into something Syspeace can work with, it is creating an **observation**, and when it passes it into the Syspeace engine and Syspeace holds onto it, it is **recording** that observation.

Using more detectors

There are many sources of login attempts in a server. A web server might have a number of web sites/applications which each have their own login system. Some login systems are patched through to Windows login, like for Outlook Web Access, but most are not. These web applications may be the primary source of attack attempts and be more, or just as, important to secure as other services like Remote Desktop or file shares.

For this purpose, Syspeace has a **Detector Provider API** (Application Programming Interface). This means that even if Syspeace does not include a detector, someone else can program a detector and ask Syspeace to load this detector. A provider is the package of files that Syspeace loads to use the detector or detectors it provides.

Programming a detector requires knowledge of C# and the .NET platform. Samples are available, and one sample in particular is a fully functional detector that does not require programming an entire detector to set up and that can solve the web login problem mentioned above.

The web detector

Syspeace provides the **Web detector** as a usable sample. It protects web applications hosted on the same server as a Syspeace installation. Here's how it works:

1. Identify which web application you want to protect. Each web application must be paired with a **Web detector reporter** component to send information about login attempts to the Web detector installed in Syspeace.
2. Download and install the Web detector reporter that fits the exact web application or the technology the web application is based on. This might involve reconfiguration or writing small bits of code. If you are using technology that Syspeace does not provide a fitting reporter for, you may have to supply your own code for this. Instructions are provided.
3. Repeat steps 1 and 2 for every web application you want to be protected.
4. Download and install the Web detector into Syspeace. The Web detector will listen for information about login attempts sent from the various Web detector reporters.

5. Start Syspeace and configure appropriate rules.
6. Try making test login attempts and verify that they are being recorded in the Access log settings pane.

Due to the way the Web detector reporters work, other web sites running on the same server would be able to report login attempts. To prevent this, you can configure a **reporting token** – a short password-like piece of text – in the Syspeace settings as well as the configuration of the individual Web detector reporters. This disallows other web sites from reporting login attempts unless they also pass in the correct reporter token.

Note that login attempts will not be able to be reported from computers other than the same server Syspeace is running on, regardless of the use of reporter tokens.

Your own detector

The Web detector involves an extra moving part to allow it to collect the data it needs, but not every detector has to be that complex. You can build a simple detector that reads from any source of login attempts you have access to, as long as you can program it. For more information, see the **Syspeace Detector Providers for Developers** document.

Installing a detector provider

To install a detector provider:

1. Go to the Syspeace installation folder.
   By default, this is **C:\Program Files\Treetop\Syspeace**.
2. If necessary, create the folder **Providers**.
3. Unzip the detector provider file and copy the folder named *DetectorName***.provider** into the **Providers** folder. The folder copied should contain a file named *DetectorName***.dll**.
4. Start (or restart) both the Syspeace service and the Syspeace client.
5. If the detector has loaded, you should see an entry for its rules in the Settings window and can start configuring them.
   If the detector did not load, you should be able to diagnose the loading error by using the new Detectors settings pane.
6. Try making test login attempts and verify that they are being recorded in the Access log settings pane.