Splunk App: Windows Security Operation Center

By Russ McRee – ISSA member, Puget Sound (Seattle), USA Chapter

Join the Discussion
Connect

Prerequisites

Windows 2003, 2008, 7

Splunk (Free or Enterprise[1])

Introduction

As a volunteer handler for the SANS Internet Storm Center, I am privileged to work with some incredibly bright, highly capable information security professionals.[2] As said individuals creat e new tools or update those they maintain, I have the advantage of early awareness and access. Bojan Zdrnja's Splunk app, Windows Security Operations Center (referred to as WSOC hereafter) is a perfect example. By the time you read this a new version should be available on Splunkbas e.[3]

Bojan bought me up to speed on his latest effort via email.

The latest version of WSOC contains bug fixes (mainly minor search tweaks) along with a couple of new dashboards:

1. A dashboard for up-to-date servers with patches
2. Directory Services dashboards

The Directory Services dashboards are very useful as they show changes to objects in AD including creations, deletions, and modifications. These views are excellent for auditors.

In the future Bojan plans to add support for other products normally found in Microsoft environments, including infrastructure elements such as DNS/DHCP, IIS, SQL server, and perhaps TMG. WSOC's primary purpose is to cover all potential security views an auditor or information security personnel might want purview of; there'll be no run-of-the-mill operational monitoring here ;-).

Bojan offered many favorite use cases. People are not always aware of what's going on in their Windows environments. In almost every implementation he's encountered, he found automated tools/services filling logs in abundance. As an example, when the tool tries to access a resource automatically, it generates an AD authentication failure event and then it successfully authenticates through NTLM. This causes logs to grow substantially. The same dashboards can be used to easily spot infected machines or brute force attacks on the network, thanks to Splunk's excellent visualization capabilities. WSOC includes a table that shows a distinct count of failed login attempts per username per machine, so if a machine is brute forcing, even if it's slow, you'll be able to see it.

Auditors are particularly fond of the user/group management dashboards. They produce ready evidence, in one view, of which users were added to which group. When coupled with change requests, yours becomes an organization that is then better prepared for audits.

The dashboard showing installed services supports this well, too, as any installed service should have an accompanied change request (see further discussion below).

Bojan wanted to stress the missing patches dashboard as extremely valuable. This information is collected from the local Windows Update agent on every server. Of course, in order for it to be accurate, the Windows Update agent must be able to connect to WSUS or Microsoft's update server; but assuming it can, results will populate nicely showing servers that have missing patches and those that are all up to date.

Windows Security Operation Center installation

You'll need a Splunk installation to make use of WSOC. I'll assume you have some familiarity with Splunk and its installation. If not, ping me via russ at holisticinfosec dot org, and I'll send you copy of a detailed Splunk article I wrote for *Admin* magazine in June 2010. You can also make use of the extensive online Splunk documentation resources.[4]

A panoply of Splunk application goodness is available on the Splunkbase site, WSOC included.[5] For the easiest installation method, from the Splunk UI, click *App* | *Find More Apps…*, then search *Windows Security Operations Center* followed by clicking the *Install Free* button.

Alternatively if you've acquired the `.tar.gz` for the app you can, again via the Slunk UI navigate to *App* | *Manage Apps…* | *Install app from file* and select the app from the location you've downloaded it to. Installation is also possible from the Splunk CLI.

1 http://www.splunk.com/download?r=header.
2 http://isc.sans.edu/handler_list.html.
3 http://splunk-base.splunk.com/apps/.
4 http://docs.splunk.com/Documentation.
5 http://splunk-base.splunk.com/apps/24435/windows-security-operations-center.

Once installed WSOC will present itself from the Splunk menu under *App* as Windows Security Operations Center. Once you've navigated to the WSOC app, options will include:

- About
  - Includes top sending servers, top source types, and contributing Domain Controllers (if applicable)
- Login Events
  - Includes Active Directory, NTLM, and RDP successful and failed attempts
- Directory services
  - Access and changes
- User management
  - User Account and Group Management
- Change Control
  - Advanced Activity Monitor
  - Windows Installations and Patch Status Overviews
  - Process Tracking
  - Time Synchronization
- Windows firewall
  - Configuration changes
  - Allowed and blocked connections
  - Allowed and blocked binds
- Saved Searches
  - Preconfigured queries, too plentiful to list
- Search
  - Standard Splunk search UI

You've got to remember to set your audit and logging policies to be sure they capture the appropriate level of success and failure in order to be properly indexed by Splunk from the security event log.[6] Recognize the profound differences between Window Server 2003 and 2008 with special attention to Event IDs. WSOC is largely optimized for Windows 2008/7 event types, but can be tuned for older versions if you know how to manage Splunk app configurations and query parameters.

6 http://splunk-base.splunk.com/answers/26958/what-to-log-for-security.

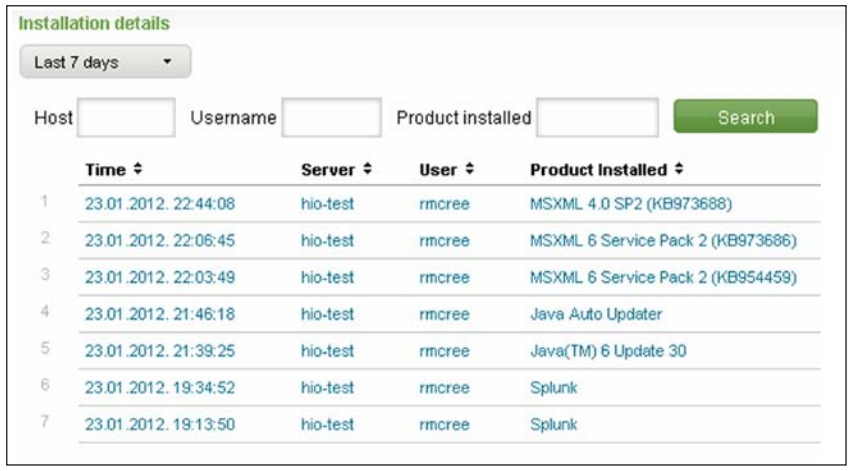

Figure 1 – WSOC Windows installation details

Remember too that you can configure Splunk as a light forwarder (CLI only) on target Windows servers and send all events to a core Splunk collector running WSOC, thus aggregating all events in one index and UI. Note the 500MB a day limitation on the free version of Splunk.

Using Windows Security Operations Center

I ran WSOC through its paces on a Windows Server 2003 virtual machine image that I literally had not touched in two years (prior snapshot: 9/11/09). With WSOC and Splunk installed I patched the VM and generated a number of different logon events via RDP and locally. I also made changes to users and groups as well as updated browsers, Flash, and Java.

WSOC smartly reported on all related activity.

Under *Change Control* | *Windows Installation Overview* I noted all installations that wrote to the security event log (the default WSOC monitored log source) as seen in Figure 1.

As configured out-of-the-box, if an event is not written to the security event log WSOC will not pick it up. As Bojan said, this app is intended as a security auditor's tool as opposed to an operational health tool.

The default search covers the last seven days from query time, but the chronology drop down menu offers a range from *15 minutes* to *All time*. Licensed versions of Splunk can also leverage real-time reporting.

Figure 2 – WSOC user account monitoring

Figure 3 – Ima Hacker bagged and tagged

Process Tracking is also a great view to monitor on critical servers. Unwelcome or unfamiliar processes may jump out at you particularly if you've baselined normal expectations for your systems.

I am currently not running Active Directory or a domain controller in my lab, which left a lot of WSOC functionality testing off the table (Directory Services, etc.), but that should not preclude you from doing so. Via *Local Users and Groups* I added an evil user, deleted some users created during testing on the VM in 2009, and deleted a couple of non-essential groups. Evidence of the activity immediately presented itself via *User management* | *User Account Management* and *Group Management* as seen in Figure 2.

It's a tad unseemly for WSOC to label UI panes as *Added Windows Domain accounts* and *Deleted Windows Domain accounts* given that the activity was local account specific, but you get the idea.

If you drill into View results, you'll receive all the detail not immediately available in the preliminary app pane. Figure 3 shows WSOC nabbing me for having created the user Ima, short for Ima Hacker. ☺

I love the *Saved Search* feature and ran *Windows – Server restarts* for you as an example, knowing I'd intentionally triggered one of those events. Results are noted in Figure 4 where you can see the fact that the reboot was spawned by Internet Explorer (Windows Update).

Lastly, the *Advanced Activity Monitor*, under *Change control*, offers search capacity via unique identifiers. In Figure 5, you'll see all the *New added services* attributed to my user account.

I did some customization of the app to capture Windows Server 2003 Windows Firewall-related events, but be aware that by default the app checks events 4946, 4947, 4948, 5156, 5157, 5158, and 5159 (Windows Server 2008 Event IDs). Enable Audit MPSSVC Rule-Level Policy Change[7] on Windows 7 and 2008 for this to capture Window Firewall events correctly. Windows 2003 Event IDs are a different event code hi-

7 http://technet.microsoft.com/en-us/library/dd772750(WS.10).aspx.

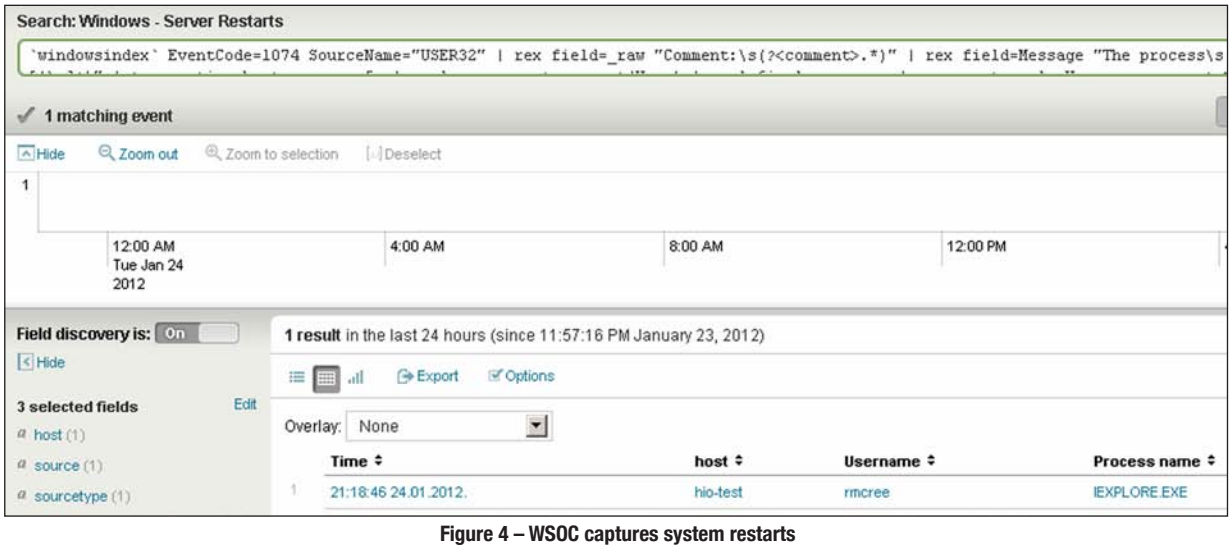

Figure 4 – WSOC captures system restarts

Figure 5 – WSOC shows added services

erarchy that is not covered by WSOC but is easy enough to customize for if you're still running 2003.

I imagine you can see the value in WSOC, particularly from an audit and awareness perspective. The nice thing about Splunk apps is they can be enhanced and built upon with relative ease. Bojan and team also offer a supported, licensed version, so that's an option for you as well.

In conclusion

WSOC is slick, particularly for teams already making use of Splunk. Once (or if) you're comfortable with Splunk, you'll find that apps such as WSOC and others make it invaluable for centralized, correlated data.

Again, if you want to read deeper dives into the power of Splunk and apps, ping me via email if you have questions (russ at holisticinfosec dot org).

Cheers…until next month.

Acknowledgements

—Bojan Zdrnja, project lead, INFIGO IS

About the Author

Russ McRee, GCIH, GCFA, GPEN, CISSP, is team leader and senior security analyst for Microsoft's Online Services Security Incident Management team. As an advocate of a holistic approach to information security, Russ' website is holisticinfosec.org. Contact him at russ at holisticinfosec dot org.