One of the action items from last week was to look into ways to get Windows events into splunk.

I found several useful websites related to windows powershell and also splunk specific stuff.

I've attached a pdf of how to configure splunk enterprise to connect to a remote windows server and extract items from the event log.

I'm not sure if this will work with our version of splunk or if it will work with a non-server windows machine but I thought I would pass it along.

I'm not that familar with powershell but the information look useful.

Links below:

Powershell

[https://www.whatsupgold.com/blog/use-powershell-automate-log-reviews](https://nam02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.whatsupgold.com%2Fblog%2Fuse-powershell-automate-log-reviews&data=04%7C01%7Ctim.preuss%40minnesota.edu%7Cf7d367e9aff14b09597008d881bfb1c2%7C5011c7c60ab446ab9ef4fae74a921a7f%7C0%7C0%7C637402007810993874%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=rpDPbt1H5sDNfGNF3RkM1wRvSmJFGEVguZv2vT%2Be1Dc%3D&reserved=0)

[https://blog.ipswitch.com/understanding-powershell-toolmaking?\_ga=2.238634432.1943267375.1604411176-817227006.1604411176](https://nam02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fblog.ipswitch.com%2Funderstanding-powershell-toolmaking%3F_ga%3D2.238634432.1943267375.1604411176-817227006.1604411176&data=04%7C01%7Ctim.preuss%40minnesota.edu%7Cf7d367e9aff14b09597008d881bfb1c2%7C5011c7c60ab446ab9ef4fae74a921a7f%7C0%7C0%7C637402007810993874%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=NW6O2aSYr0BS8hme%2BvEaBDiBawkToUxYqanWDbzutEM%3D&reserved=0)

[https://docs.microsoft.com/en-us/powershell/scripting/learn/ps101/00-introduction?view=powershell-7](https://nam02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fpowershell%2Fscripting%2Flearn%2Fps101%2F00-introduction%3Fview%3Dpowershell-7&data=04%7C01%7Ctim.preuss%40minnesota.edu%7Cf7d367e9aff14b09597008d881bfb1c2%7C5011c7c60ab446ab9ef4fae74a921a7f%7C0%7C0%7C637402007811003867%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=CyCISkwiyIJ6LR7pwWD3fAxmqBCkoC1gK0JXKOJehrg%3D&reserved=0)

[https://kb.webspy.com/s/article/windows-event-logs-and-powershell](https://nam02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fkb.webspy.com%2Fs%2Farticle%2Fwindows-event-logs-and-powershell&data=04%7C01%7Ctim.preuss%40minnesota.edu%7Cf7d367e9aff14b09597008d881bfb1c2%7C5011c7c60ab446ab9ef4fae74a921a7f%7C0%7C0%7C637402007811003867%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=Qhjht45%2F1tI2Hx5h7JyE8ijXK%2BIO4bNHkQ0HqzZX8pU%3D&reserved=0)

[https://blog.netwrix.com/2015/11/06/windows-event-log-forwarding-with-powershell/](https://nam02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fblog.netwrix.com%2F2015%2F11%2F06%2Fwindows-event-log-forwarding-with-powershell%2F&data=04%7C01%7Ctim.preuss%40minnesota.edu%7Cf7d367e9aff14b09597008d881bfb1c2%7C5011c7c60ab446ab9ef4fae74a921a7f%7C0%7C0%7C637402007811013861%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=T5NsZ%2B0cjkhqgwuvRw6i%2FiNqBiUr8aqy0Tsxg3dzl%2Bc%3D&reserved=0)

Splunk

[https://splunkbase.splunk.com/app/3067/#/overview](https://nam02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsplunkbase.splunk.com%2Fapp%2F3067%2F%23%2Foverview&data=04%7C01%7Ctim.preuss%40minnesota.edu%7Cf7d367e9aff14b09597008d881bfb1c2%7C5011c7c60ab446ab9ef4fae74a921a7f%7C0%7C0%7C637402007811013861%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=Xb0pq%2BkRgfB2STODmgqvorTyRuXB53fSlcWAh90WfY8%3D&reserved=0)

[https://community.splunk.com/t5/All-Apps-and-Add-ons/How-do-I-collect-basic-Windows-OS-Event-Log-data-from-my-Windows/m-p/440187](https://nam02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcommunity.splunk.com%2Ft5%2FAll-Apps-and-Add-ons%2FHow-do-I-collect-basic-Windows-OS-Event-Log-data-from-my-Windows%2Fm-p%2F440187&data=04%7C01%7Ctim.preuss%40minnesota.edu%7Cf7d367e9aff14b09597008d881bfb1c2%7C5011c7c60ab446ab9ef4fae74a921a7f%7C0%7C0%7C637402007811023853%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=CiSn9QkSNif5%2Bohp%2F31RO5q%2FGVbezoobm%2FXiSUPZmiY%3D&reserved=0)

[https://docs.splunk.com/Documentation/Splunk/latest/Data/MonitorWindowseventlogdata#Collect\_event\_logs\_from\_a\_remote\_Windows\_machine](https://nam02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.splunk.com%2FDocumentation%2FSplunk%2Flatest%2FData%2FMonitorWindowseventlogdata%23Collect_event_logs_from_a_remote_Windows_machine&data=04%7C01%7Ctim.preuss%40minnesota.edu%7Cf7d367e9aff14b09597008d881bfb1c2%7C5011c7c60ab446ab9ef4fae74a921a7f%7C0%7C0%7C637402007811023853%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=trF9Zowutp88z1ypsP7j%2FiM3WUt9%2BOCpcv86OHK7Wvc%3D&reserved=0)

Dave Christianson