Microsoft: Windows security

Microsoft Windows security logs are records of information related to login attempts (success and failure), elevated privileges, directory service access, policy changes, privilege use, and other security events, as defined in a system's audit policy. These logs are one of the primary tools used by system administrators to detect and investigate unauthorized activity and to troubleshoot system problems. There are over 400 loggable events. We recommend following Microsoft’s official guidance for “Stronger” security visibility. The Audit Policy Recommendations page from Microsoft TechNet provides detailed configuration settings per operating system from Windows 7 / Server 2008 and later. In the Common Information Model, Windows security log data can be mapped to any of the following data models, depending on the field: Authentication, Performance, Updates, Vulnerabilities, Endpoint, Event Signatures, and Change.

Configuration

Guidance for onboarding data can be found in the Spunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). Refer to the documentation, and note the following:

- Recommended index: oswinsec
- Source type: wineventlog:security
- Input type: WinEventLog://Security
- Add-on or app: Splunk Add-On for Microsoft Windows
- Sizing estimate: Ranges can vary dramatically. For example, with highly active Active Directory controllers with thousands of simultaneous users, you could see more volume. At a very high level, common ranges are:
  - Workstation: 4-6 MB/day (Including Application, System, and Security Logs)
  - Application Servers: 25-50 MB/day
  - Domain Controllers: 50-500 MB/day depending on the number of users

If you have already started ingesting the data sources into another index, then you can usually proceed, though you should consider whether you should separate Windows Security logs from Process Launch Logs and both from Application and System logs, based on who likely will need access or be prohibited access. If you have already started ingesting data with a different sourcetype, we recommend that you switch over to the standardized source types.

Validation

When deploying audit policies, usually new systems or an increase in system log messages show up first in Splunk. If you already have some logs coming in and want to validate that you’re getting the new ones, look for the delta between your old policy and your new one, and Google “Windows Event ID” – that will usually give you something specific to search for (though you may have to take the action that gets logged, if it’s less common). A good example is “Windows Process Creation Event ID,” which quickly nets you “Event ID 4688” as the first result.
Application

When your Splunk deployment is ingesting Windows security logs, you can use the data to achieve the following:

- Recognizing improper use of system administration tools
- Monitoring Windows account access
- Detecting overly permissive access control lists