Log forwarding agents:

<http://nxlog.org/products/nxlog-community-edition/download>

<http://help.papertrailapp.com/kb/configuration/configuring-remote-syslog-from-windows/>

<http://sourceforge.net/projects/syslog-win32/>

<http://sourceforge.net/projects/ntsyslog/> (NT and 2k)

[http://sourceforge.net/projects/snare/](http://sourceforge.net/projects/snare/?source=typ_redirect)

Extra Reading:

<https://malwarearchaeology.squarespace.com/logging>

<http://journeyintoir.blogspot.com/2014/09/siem-use-case-implementation-mind-map.html>

<https://www.loggly.com/ultimate-guide/logging/linux-logging-basics/>

<http://lkhill.com/nxlog-convert-to-syslog/>

<http://www.slideshare.net/Hackerhurricane/windows-logging-cheat-sheet-v11>

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx> (Windows Event Id lookup)

<https://www.owasp.org/index.php/Logging_Cheat_Sheet>

<https://zeltser.com/security-incident-log-review-checklist/> (scour his site, he has some good info)

<https://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528>

<https://www.sans.org/reading-room/whitepapers/logging/detecting-security-incidents-windows-workstation-event-logs-34262>

<https://download3.vmware.com/vcat/vcat31_documentation_center/index.html#page/Operating%20a%20vCloud/3b%20Operating%20a%20VMware%20vCloud.2.087.html>

<https://www.alertlogic.com/downloads/AL_Configuring-Log-Sources-Best-Practice.pdf>

<http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf>

[http://blog.sematext.com/2015/07/21/coreos-clusters-centralized-log-management-and-monitoring](http://blog.sematext.com/2015/07/21/coreos-clusters-centralized-log-management-and-monitoring/)

<https://www.reddit.com/r/AskNetsec/comments/2qppto/siem_correlation_rule_repository/?sort=top>

---------------------------------------------------------------------------------------

Not as common windows log sources

C:\Windows\Logs\CBS\cbs.log (windows vista/2008+ package manager logs) https://support.microsoft.com/en-us/kb/928228

C:\Windows\inf\setupapi.\*.log contains install records for devices (including thumb drives), service packs, and hotfixes

Windows firewall logs (pfirewall.log)

Windows malicious software removal tool logs C:\Windows\debug\mrt.log