Intro to Splunk Resources

(These resources are not necessarily referenced in the class, but will be a big help as you learn Splunk)

Splunk Website References

Splunk Documentation: https://docs.splunk.com/Documentation/

Splunk Answers: https://answers.splunk.com/index.html

- @splunkanswers on Twitter

Splunkbase: https://splunkbase.splunk.com/

Splunk Certifications & Training: https://www.splunk.com/en_us/training.html

REST API Tutorials: https://docs.splunk.com/Documentation/Splunk/7.2.5/RESTTUT/RESTsearches

Splunk Search Manual:
https://docs.splunk.com/Documentation/Splunk/7.2.5/Search/GetstartedwithSearch

Splunk Search Tutorial:
https://docs.splunk.com/Documentation/Splunk/7.2.5/SearchTutorial/WelcometotheSearchTutorial

SPL reference:
https://docs.splunk.com/Documentation/Splunk/7.2.5/SearchReference/WhatsInThisManual

Pivot manual: https://docs.splunk.com/Documentation/Splunk/7.2.5/Pivot/IntroductiontoPivot

Search Reference: https://docs.splunk.com/Documentation/Splunk/7.2.5/SearchReference/Search

Command quick reference:
https://docs.splunk.com/Documentation/Splunk/7.2.5/SearchReference/ListOfSearchCommands

Search commands by category:
https://docs.splunk.com/Documentation/SplunkLight/7.2.5/References/Searchcommandsbycategory

Planning your environment

Capacity Planning Manual:
https://docs.splunk.com/Documentation/Splunk/7.2.4/Capacity/IntroductiontocapacityplanningforSplunkEnterprise
Splunk Storage Sizing: https://splunk-sizing.appspot.com/
Splunk Enterprise Installation Manual:
https://docs.splunk.com/Documentation/Splunk/7.2.5/Installation/Whatsinthismanual

Data References

Monitoring files and directories:
https://docs.splunk.com/Documentation/Splunk/7.2.5/Data/Monitorfilesanddirectories
Getting data from TCP and UDP ports:
https://docs.splunk.com/Documentation/Splunk/7.2.5/Data/Monitornetworkports
Monitoring Windows event log data:
https://docs.splunk.com/Documentation/Splunk/7.2.5/Data/MonitorWindowseventlogdata

Splunk Community

Request to join the Splunk-Usergroups Slack:
https://docs.google.com/forms/d/e/1FAIpQLSd2PXSBiatZvCIpdE2wPFgnrUM29HBYjrkI0iDhlx26RwwE4A/viewform
Join Splunk Bucketlist: https://bucketlist.splunk.com
Splunk User Groups: https://usergroups.splunk.com/

Use-Case Examples

12 Days of Splunk Use Cases: https://www.splunk.com/blog/2018/12/06/12-days-of-splunk-use-cases.html
Splunk Enterprise Security Use Cases:
https://docs.splunk.com/Documentation/ES/5.2.2/Usecases/Overview
Predictive Maintenance:
https://www.splunk.com/blog/2019/02/25/applying-machine-learning-to-maintenance-operations.html
Selling Girl Scout Cookies: https://www.splunk.com/blog/2018/02/27/thin-mints-samoas-and-splunk.html
Security Use Cases from InfoSec Institute:
https://resources.infosecinstitute.com/wp-content/uploads/Security-Use-Cases-using-Splunk.pdf

Searching

LearnSplunk.com Search Tutorial: https://www.learnsplunk.com/splunk-search-tutorial.html
CloudiBee Search Cheatsheet: https://www.cloudibee.com/splunk-search-cheatsheet/
GoSplunk (for examples of searches submitted by users): https://gosplunk.com/

Apps of Interest

Splunk Essentials

There are many Splunk Essentials apps available. Search Splunkbase to see what is most applicable to your use case.
Splunk Security Essentials: https://splunkbase.splunk.com/app/3435/
Splunk Essentials for Wire Data: https://splunkbase.splunk.com/app/4372/
Splunk Essentials for ICS Monitoring and Diagnostics: https://splunkbase.splunk.com/app/4287/
Splunk Essentials for ICS Security and Compliance: https://splunkbase.splunk.com/app/4150/

Other Apps

Some other apps that may be of interest. These have not necessarily been vetted but give you an idea of what is available in Splunkbase.
InfoSec App for Splunk: https://splunkbase.splunk.com/app/4240/
DDoS Detector for Splunk: https://splunkbase.splunk.com/app/4016/
G Suite for Splunk: https://splunkbase.splunk.com/app/3791/
Microsoft Office 365 App for Splunk: https://splunkbase.splunk.com/app/3786/
Splunk App for AWS: https://splunkbase.splunk.com/app/1274/

Resources for further study

Breaking Down Incident Response Podcast, Episode 6 (Covers dealing with SIEMs):
https://www.imfsecurity.com/podcasts/2018/8/26/bdir-podcast-episode-006
Splunk Threat Hunting Blog:
https://www.splunk.com/blog/2017/07/06/hunting-with-splunk-the-basics.html
Splunk Security Sandbox: https://www.splunk.com/page/sign_up/es_sandbox
Splunk User Behavior Analytics Course:
https://www.splunk.com/en_us/training/courses/user-behavior-analytics.html
Boss of the SOC:
https://www.splunk.com/blog/2018/05/25/boss-of-the-soc-bots-investigation-workshop-for-splunk.html

- App: https://splunkbase.splunk.com/app/3985/

Security Datasets Project: https://live.splunk.com/splunk-security-dataset-project
Splunk 'N Box: https://conf.splunk.com/files/2017/slides/splunk-n-box.pdf