Introduction to Splunk

Module 4: inputs.conf

Natasha Staples

CYBRARY

In this video:

- About configuration files
- Monitor file location using inputs.conf
- Configure receiving

CYBRARY

Configuration files:

- Settings, authentication information, save searches, etc.
- Ends in .conf
- Written in stanzas
- Splunk often needs restarted after changes

```
[tcpout]
indexAndForward=true
compressed=true

[tcpout:my_indexersA]
compressed=false
server=mysplunk_indexer1:9997, mysplunk_indexer2:9997
```

CYBRARY

Inputs.conf

- $SPLUNK_HOME/etc/system/local

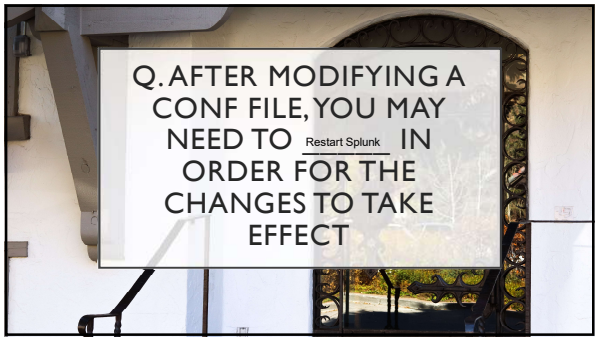
```
[monitor://<path>]
index =
sourcetype =
```

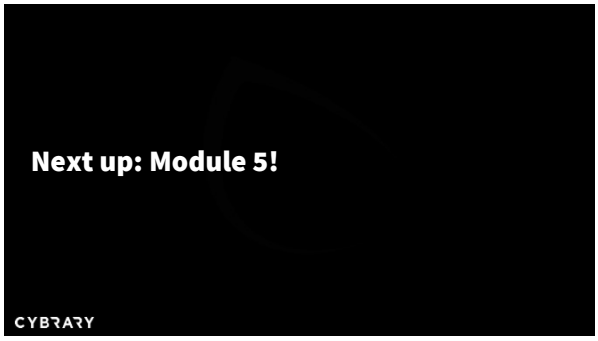
CYBRARY

Configure receiving

- On Splunk Web Interface
- Server Settings Check
- Listen on port 9997

CYBRARY




Next up: Module 5!
CYBRARY