Splunk4Rookies -
Splunk Connect for Syslog (SC4S)

Hands-on Splunk Workshop

What is Splunk4Rookies - Splunk Connect for Syslog? Splunk4Rookies sessions are a great opportunity for you to discover the value of Splunk hands-on in a matter of hours. Attendees will learn how to collect, analyse and visualise syslog data with Splunk.

Content: During the workshop you will learn the foundations of deploying and configuring the Splunk Connect for Syslog (SC4S) container and will receive guidance on collecting syslog data at scale. You will then search analyse and visualise that data within Splunk.

Target Audience: Sessions are designed for Splunk beginners who are interested in onboarding and analysing syslog data.

Prerequisites: None, other than an open mind and a willingness to learn!

Delivery Method: Workshops are currently delivered both face to face and virtually, so anyone can join regardless of location! Ask your Splunk account manager for more information.

Goals/Outcomes: Attendees will leave with sufficient understanding of podman, containers and Splunk Connect for Syslog (SC4S) to start deploying the solution.
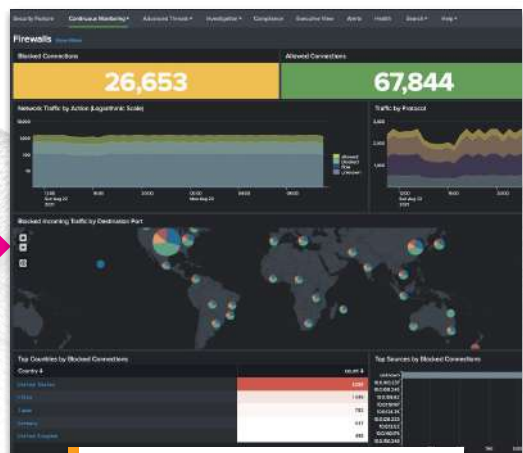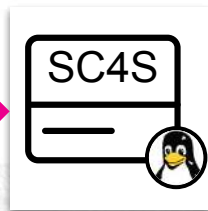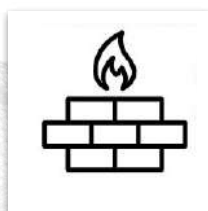
Duration: Workshops typically last around 3 hours

What Do I Need to Bring?
● A web browser with Internet access to connect to a Splunk server via port 443 (Test your connectivity here: https://domain-test.splunk.show.)
● A splunk.com account to login to the workshop environment (create an account here).

Onboard syslog data…

…then analyse and visualise it in Splunk!

splunk> turn data into doing