Splunk4Rookies - Security

Splunk & Learn!

What is Splunk4Rookies - Security? Hosted by our Sales Engineering team, these sessions are a great opportunity for you to discover the value of Splunk hands-on in a matter of hours. Attendees get an introduction to Splunk, along with hands-on experience detecting and investigating a security incident and creating a dashboard to detect future incidents

Content: During a session, we will walk through a series of exercises designed to get someone new to Splunk to the point where they understand what Splunk is and what it is capable of. Attendees will analyse security data to detect malicious behaviour, then create a dashboard to detect the nefarious activity to prevent it happening again.

Target Audience: Sessions are designed for Splunk beginners. Whether your organisation is just starting to consider using Splunk or you have just joined a team of Splunk Ninjas and need to understand the basics, Splunk4Rookies - Security is for you!

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

Delivery Method: Splunk4Rookies - Security events are typically run either in person or virtually directly to you, the users. Ask your Splunk account manager for more information!

Goals/Outcomes: Attendees will gain a good understanding of the value Splunk delivers, particularly in security analytics and detections
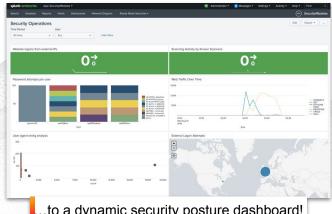
Duration: Workshops typically last between 2½-3 hours

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

Go from messy security data…

…to a dynamic security posture dashboard!

splunk> turn data into doing