Pubcast - Splunking Data!

Monday, 01 June 2009

Episode 11 of the IT Security Pubcast.

The Pubcast examines a free tool to collate and correlate log data from different sources in order to provide a meaningful management view of risk.

While application and system logging is a core security requirement it is often overlooked for numerous reasons: the logs are disseminated around the organisation, they are overwritten before they can be utilised, they take space, they are seldom considered aside from forensic analysis, and it can be difficult to correlate the different events they represent. In short, this core security asset is often overlooked because of the cost and complexities of utilising it.

The Pubcast discussed this with Stefan Buys and Marinus van Aswegen, who are working with SPLUNK, a free solution that collates data from multiple sources, stores it and provides elegant mechanisms to interpret it. The debate considers and how a where a tool like this would be best implemented, whether the average security practitioner has the ability to do so, and the all important question of support.

Pubcast Episode 11 (Full)

Download the Full Audio File

{audio}http://www.discussit.co.za/_media/_audio/itsp/pce11.mp3{/audio}

Pubcast Episode 11 (Part 1)

{audio}http://www.discussit.co.za/_media/_audio/itsp/Pubcast_Episode_11_1.mp3{/audio}

Pubcast Episode 11 (Part 2)

{audio}http://www.discussit.co.za/_media/_audio/itsp/Pubcast_Episode_11_2.mp3{/audio}

Pubcast Episode 11 (Part 3)

{audio}http://www.discussit.co.za/_media/_audio/itsp/Pubcast_Episode_11_3.mp3{/audio}