A new approach to detection and triage

Douglas Brown[1]
[1]*Red Hat*

In this session, we will challenge the notion of a false-positive, showing how auto-closed alerts that measure change and aggregate risk are the most effective means of detecting unknown threats, raising actionable alerts and reducing alert fatigue. We will also provide a 5 step process for the development of change-based detection techniques and a new taxonomy for their classification, enabling higher-order meta-analysis.