https://prezi.com/k_tnpyseherj/siem-summit-2017-actionable-detects/