TITLE (20 words maximum)

Better SOAR than Sorry

ABSTRACT CONTENT (300 words)

Is more information always better? What is the point of information if you don't act on it? Will information quickly become stale if we don't act on it in a timely manner? These are some of the questions USQ's Cyber security team have been grappling with while managing an in house SIEM for the past 6 years. While visibility of what is happening or could happen in your environment is ideal, responding manually and quickly every time becomes overwhelming and unsustainable. To have a fighting chance at winning as a defender, we need to do what the attackers are doing: automate our responses as much as possible.

This presentation examines these challenges at USQ where it quickly became impossible for a small team to respond to multiple incidents in a timely and consistent manner. USQ's solution was to leverage an existing investment in Splunk Enterprise and Enterprise Security, with the deployment of Splunk Phantom - a SOAR (Security Orchestration Automation and Response) platform to enable fast and reliable responses to security events. All integration points will be discussed as well as the target use cases and corresponding playbooks. Playbooks examined will include triaging compromised accounts, responding to reported phish and responding to third party threat intelligence.