What to Follow? The Sun or the Stars

Kevin Garvey
Manager – Incident Response and Threat Management
Time Warner Corporate
The price of doing the same old thing is far higher than the price of change. --Bill Clinton
Background

• Cyber Security for four years and eight in IT
• SIEM administrator for four years as well as an administrator of other cyber security toolsets
• Worked with many different groups within IT to help develop better relationships with Cyber Security
• Metrics is just as important to my job as finding the adversary
Way Too Many Challenges

• Way too many alerts for most SOCs
• Way too much time performing tuning exercises
• Way too much time doing operational related items
• Way too many decisions on what logs need to be ingested
Risk Based Approach

• What are your privileged assets? What else should you look at?
• Are you focusing on the right items?
• Would the bad actors be going after the same assets?
• Focus on what other SOCs may not be focusing on
Processes and Procedures

• No one has ever been fired for following processes and procedures

• No bad actor has ever called us asking for processes and procedures!

• Go far beyond processes and procedures to shoot for the stars!
Runbooks

• Do you have runbooks?
• If you do, when was the last time the run books were reviewed?
• Should SOC analysts look past a runbook?
Shooting for the Stars!

• How does your SOC give the extra 10%?
• Following frameworks that are hard to capture in processes/procedures or runbooks such as MITRE.
• Sharing finding with other industry aligned threat intelligent groups.
The art of life is a constant readjustment to our surroundings. --Kakuzo Okakaura