Tuesday, June 25, 2024

2:50 PM - 3:10 PM

KPIs Or It Didn't Happen: Cyber Threat Intelligence Metrics and Efficacy

Jason Baker

Threat Intelligence Consultant, Research and Intelligence Team (GRIT)

GuidePoint Security

Abstract:

Despite entering our lexicon nearly two decades ago, objective measurements and metrics of Cyber Threat Intelligence (CTI) remain ambiguous, highly variable, or infrequently adopted. This inconsistency is in part due to varying business and information needs that drive disparate CTI programs, our failure to adopt a universal standard, and an occupational culture that frequently "falls back" on US Intelligence Community (USIC) practices in lieu of independent doctrine. This presentation will seek to review contemporary CTI metrics and their underlying purpose, identify deviations from USIC practices, explain common pitfalls that lead to issues in evaluating program efficacy, and review the "lifecycle" of CTI metrics in organizations of varying maturity levels. Attendees will leave with reliable measures to evaluate CTI program efficacy, awareness of issues to avoid, and be empowered to pursue contemporary approaches to metrics, evaluation, and CTI program management. To begin, we will present CTI metrics as a subcomponent of evaluation and feedback within the intelligence cycle and how they are applied to traditional intelligence community all-source intelligence. We will separate the form and function of CTI from that of the USIC, and explain how this disparity leads to issues in tracking and actionability of common CTI metrics. Next, we will explore best practices in CTI metrics as key performance indicators, measures of effectiveness, and measures of performance, with examples of how organizations can develop the complexity of their metrics over time. We will present metrics as a "ground-up" component of CTI programs and provide examples of "baking in" metrics and tracking mechanisms from program establishment through to full operational maturity. Finally, we will close with case studies that reflect the "lifecycle" of metrics, from intelligence requirements, through intelligence production, and finally in documentation and evaluation. This portion will provide examples of both quantitative and qualitative evaluation as well as subsequent program modifications that they may inform.