Mark Underwood

The Quality "Logs"-Jam: Why Alerting for Cybersecurity is Awash with False Positives, Missing Data and Inscrutable Dashboards

What happens when the (Observe) Plan-Do-Check-Adjust cycle is undermined by lapses in data integrity? Observations are questioned. Plans may be ill-conceived. Actions may be undertaken that undermine rather than enhance. "Checks" can fail. Adjustments may be guesswork. In cybersecurity, the results of poor data integrity can be expensive outages, ransom requests, breaches, fines -- even bankruptcy (think Cambridge Analytica). But data integrity issues take many forms, ranging from benign to malicious. The full range of these issues is surveyed from a cybersecurity perspective, where logs and alerts are critical for defenders -- as well as quality engineers. Techniques borrowed from model-based systems engineering and ontology AI to are identified that can mitigate these deleterious effects on PDCA.