FACULTY CANDIDATE PRESENTATION

Dynamic Optimization of the Level of Operational Effectiveness of a Cybersecurity Operations Center.

-Ankit Shah, Ph.D.

Biography

Ankit Shah received the B.S. degree in computer science from Florida Atlantic University, Boca Raton, FL and the M.S. degree in operations research from George Mason University, Fairfax, VA, where he is a Ph.D. candidate in the interdisciplinary program amalgamating principles from operations research and computer science with the Volgenau School of Engineering. His research interests include cybersecurity, predictive and prescriptive analytics, decision making under uncertainty, combinatorial optimization, and stochastic dynamic programming with reinforcement learning. He has authored or coauthored ten articles in refereed journals and conference proceedings (IEEE, ACM, and Springer) and three book chapters in the application area of cybersecurity. He has served as a reviewer for security conferences and a session chair for security analytics at the INFORMS optimization 2018 conference. He has been invited for more than twelve technical talks and seminars by government organizations, industry partners, and technical conferences.

UNIVERSITY OF SOUTH FLORIDA

Abstract

A cybersecurity operations center (CSOC) through a unique combination of people, processes, and technology, protects organizations against the ever-increasing cybersecurity threats. Analysts, working in shifts, help in detecting, analyzing, and reporting significant alerts that are generated by the intrusion detection systems (IDSs). Under normal operating conditions, sufficient numbers of analysts are available to analyze the alert workload in a reasonable amount of time. However, many disruptive factors can adversely impact the normal operating conditions such as higher alert generation rates from a few IDSs, new alert patterns that decrease the throughput of the alert analysis process, analyst absenteeism, and internal system failures. The impact of all the above factors is that the alerts wait for a long duration before being analyzed, which impacts the readiness of the CSOC. In order to return the CSOC to normal operating conditions, additional resources (which are limited in quantity) can be called upon to boost the investigation rate of alerts. It is imperative that (1) the readiness of the CSOC be quantified, which in this research is defined as the level of operational effectiveness (LOE) of a CSOC, and (2) (near-) optimal actions are taken to return the CSOC to normal operating conditions. First, LOE is quantified using a queueing metric and a dynamic monitoring framework is developed, which gives a color-coded representation of the LOE status. Non-trivial decisions must be made about when and how much action to take in the face of uncertainty in a resource-constrained environment. Hence, next in this research, an intelligent sequential decision-making tool using reinforcement learning (RL) framework is developed for optimizing the LOE of a CSOC under adverse conditions. The RL framework is built using the principles of stochastic dynamic programming with value function approximation. Results indicate that the RL framework is able to assist the CSOC with a decision support tool to take better actions compared to current myopic or rule-based practices, which allows for a paradigm shift in optimizing the performance of a CSOC. Finally, this talk will present a brief overview of other research problems at a CSOC and potential future research directions.