UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PhD Seminar 1

Monday February 14, 2022 at 1:30pm via Zoom

Edward Crowder

A Framework for Meta Learning Enhanced Cyber Threat Hunting with Intelligent Systems

Advisor: Dr. Ali Dehghantanha
Advisory: Dr. Hassan Khan
Advisory: Dr. Graham Taylor [Engineering]
Advisory: Dr. Mohammad Hammoudeh [Manchester Metropolitan University]

Abstract:

Cyber threat hunting is the pursuit of proactively finding unknowns in the vast ever-changing cyber threat landscape. Massive shifts in IT infrastructure such as cloud initiatives have given hackers new ways to infiltrate your organization by expanding the attack surface exponentially. Identifying new zero-day threats require advanced Human operators who can do this with relative ease using their vast knowledge and experience to pivot to new, never seen threats. The same cannot be said for conventional machine learning and narrow, deep learning systems.

This seminar will discuss the concept of meta learning or “learning to learn” in a cyber threat hunting context. The importance of meta learning in cyber threat hunting will be highlighted by addressing the conventional shortcomings and gaps of the current state-of-the-art systems. Further, we will connect the dots between the benefits of meta learning against industry-standard metrics that define a successful threat hunting program in our proposed framework.