Wednesday, June 26, 2024

2:30 PM - 2:50 PM

Transforming Security through Language Models

Jonathan Mullin, Ph.D.

Chief Technology Officer

DCI Solutions

Abstract:

The power of Generative Artificial Intelligence (GenAI) is the ability to adapt to almost any data type as long as there is enough data to build a statistical model upon which deep non-linear relationships can be established. This is a perfect for Cybersecurity applications which can generate an absolute deluge of data. Using this massive data resource learning models can create internal representations in lieu of hard labels used in traditional machine leanring. The only limitation is traditional GenAI approaches require billions of parmeters and KiloWatts of power to provide insight into cyberdata. Our approach at DCI solutions seeks to bridge the power of GenAI with a scalable architecture capable of running on device not locked away in the cloud.

CyFormer harnesses the power of Artificial Intelligence (AI) for the purpose of transforming cybersecurity. CyFormer is powered by state-of-the-art AI models to defend against never-before-seen cyberattacks at both the network and host level. CyFormer covers all aspects of the cyber threat, both from inside and outside adversaries. The basis of our stance is not to rely on known threats of the past, but to model your network to find who can be trusted now and into the future. CyFormer applies seamlessly as part of any network architecture and is a flawless technology insertion into a Zero-Trust Architecture providing visibility and analytics.

CyFormer is a signatureless agent that feeds off network data and learns what “normal” network behavior is for a customer. From there, the CyFormer model can identify activity outside the normal baseline, tag those activities, and send alerts through JSON messaging. CyFormer is custom built specifically to address the unique challenges of cyber data. Our models develop internal representations of each entity and their relationships, thus allowing a fast, scalable identification when unusual events happen. CyFormer is capable of responding independently or via teaming with security professionals through reports explaining the reasoning for the alerts. This methodology helps to build deep trust while augmenting a security team to effectively investigate the vast scale of cyber data in a meaningful, systematic, and straightforward way.

DCI is now pushing the boundary of automated cyber defenses by combining CyFormer with reinforcement learning (RL) approaches. This combination is transformative. The combination of a language model to drive and inform the actions of the RL agent allows for a dynamic interplay between each allowing for both specialization of each model and teaming with a common goal. CyFormer allowed us to move detection to the left of indicator of compromise (IOC), the combination of RL pushes remediation even further to the left denying adversaries the chance to even dwell in your environment.