Cyber offensive techniques are often asymmetric in nature, generating large amounts of noise in enterprise networks and requiring far more time to investigate than to launch. Traditional analyst tools employed by enterprise SOC teams generate thousands of alerts daily, draining analyst resources, and eroding time dedicated to digging deeper. With recent advancements in machine learning there is increased interest within the DoD to find new applications of machine learning for network defense to help level the playing field in cyberwarfare by providing direct access to ML enabled cyber tools directly to helpdesk operators for instantly identifying and remediating threats all through intelligent machine based automated workflows. While DoD organizations are interested in how machine learning algorithms can help solve their problems, they are unsure of how to integrate these technologies into their networks. Booz Allen has developed end to end automated network defense solutions integrating machine learning models for network threat detection at the edge with enterprise security orchestration, automation, and response capabilities.

In this talk we will cover our motivations, lessons learned, design considerations, future potential applications and ramifications thereof. In the development of MINDSOAR, Booz Allen has leveraged its direct DISA experience from its support of the Software Defined TMO, the Machine Learning working group and the unified collaboration office to deliver a fully automated threat detection and response capability accessible to helpdesk operators (GSD). MINDSOAR utilizes a containerized ML platform using Docker Containers and develops a continuous training environment where the models are constantly being trained and deployed and accessible to help desk operations through DISA Defense Collaboration Service (DCS) Swift chat client. Operators utilize this ChatOps capability to enable rapid collaboration with integrated tool sets. By integrating a Chatbot with DISA SWIFT Chat client and the ML platform, we were able to develop a capability that can be utilized by operators to perform proactive cyber threat hunting and take immediate remediation actions.