## $1.00 Million USA CERDEC STTR Phase II Award: Tactical Cyber Immune System. (November 2019- November 2021)

Our goal in Phase II STTR proposal is to leverage the tools and data analytics algorithms developed in Phase I to demonstrate the full functionality of the proposed Tactical Cyber Immune System (TCIS). We have developed a modular and adaptive cyber immunity system to overcome security deficiencies of current computing systems. We have developed algorithms and tools to characterize the self-behavior of “Computer”, “User”, and “Application” so that each behavior can be identified as either "Self" or "Non-Self".

The phase I results that will be leveraged are: 1) Self-behavior Model for Computers: Data analytics techniques are used to build the self-behavior model. Our results show that our approach achieved almost 100% accurate detection rate; 2) Self-behavior Model for Users: Data analytics techniques are used to build the self-behavior model. Phase 1 results show that our approach can successfully classify user normal versus malicious with accuracy more than 99%; 3) Self-behavior Model for Applications: The self-behavior model produced zero false negatives and detection accuracy was around 99.51%.

The preliminary results from Phase I research and development tasks have demonstrated the feasibility of our approach to build the proposed Tactical Cyber Immune System. Also, we showed that the data analytics approach is more accurate than other probabilistic methods, is scalable to handle large enterprise environments, and can be offered commercially as a cloud service. In Phase II, we will build a fully function TCIS prototype using AVIRTEK autonomic cyber security technology and the tools and data analytics algorithms developed in Phase I.