3:15 p.m. – 3:45 p.m.

A DevOps Strategy for Defensive Cyber Operations

Ed Sealing
CEO
Sealing Technologies, Inc.

In military operations, speed = lethality. This is true in ground, sea, air and space operations and is especially applicable in the cyber domain. Increases US force lethality in the cyber domain will improve lethality in the other domains, or perhaps even avoid conflict altogether. To achieve the potential of cyber's force multiplication, we must remove the physical barriers currently encumbering rapid deployment and operations of cyber weapons systems. SealingTech is helping DISA to tackle the challenge of improving cyber lethality and retaining US military cyber dominance. Deploying new DCO capabilities across the Enterprise is traditionally a long process. Some of DISA’s current capabilities such as JRSS, ZND-Email, Sharkseer, reside on proprietary hardware hosted in physical datacenters and take years to deploy. Coordinating the purchase, testing, installation, and integration of physical hardware appliances across the enterprise takes large amounts of resources and time. Increasing capacity often involves upgrading the proprietary hardware and licensing, requiring more network downtime. DevOps practices have been created to provide a rapid deployment pipeline for applications, but are often reserved for use in virtual or container applications, rather than proprietary appliances. In this presentation, we provide an approach for combining modern datacenter technologies in the areas of containers, virtualization, and orchestration, with the latest advancements in software defined networking, and show how this can be applied directly to network defense capabilities to streamline security tools and improve situational awareness. This approach allows for extremely rapid deployment of targeted defensive capabilities across the entire enterprise. It also changes the traditional “rip-and-replace” upgrade path of appliances and allows for horizontally scaling to add performance or storage, effectively eliminating outages due to upgrades. Utilizing commodity hardware and minimizing touch-labor drastically reduces the cost of deployment, operations, and upgrades. Over the past year, SealingTech has been designing and building an open-source reference implementation of a scalable virtualized DCO platform using the concepts and technologies mentioned above. We have tested it with well-known open-source security tools in the areas of Active defense, Passive detection, and Event Analytics. We will provide an overview of the lessons learned on how to employ this model across the DoDIN to improve speed and increase lethality.