Speakers:

- **Daniel Lohin,** Principal Security Engineer, Sealing Technologies, Inc.
- **Ed Sealing,** President and CEO, Sealing Technologies, Inc.

Managing Bro Deployments at Scale Using DevOps Technologies

This talk will discuss Sealing Technologies research of implementing Bro using modern DevOps tools including Docker, Kubernetes, and Jenkins. SealingTech has found that using these tools can be used to deploy, configure, and maintain Bro in a more efficient manner. SealingTech has worked to build an open source platform to deploy Bro and many other tools as part of this research.

Organizations are looking to utilize Bro in a manner that is easy to deploy and can be horizontally scaled to meet the growing bandwidth requirements needed. To keep up with adversaries continuously attacking networks it is necessary to be able to deploy these tools as rapidly as possible. SealingTech put together a team of top engineers and innovators to solve these challenges and asked if a DevOps approach was possible. SealingTech has been experimenting and building a platform which can be used to deploy and manage Bro using modern DevOps technologies. Using Docker containers and Kubernetes, SealingTech has been able to easily deploy Bro and manage scalability requirements. Bro is integrated into an entire architecture for gathering, parsing, and storing logs.

SealingTech will show common challenges managing Bro inside of containers, how to efficiently process traffic, how to integrate Bro with other tools such as Elasticsearch using Kubernetes, and how to build a Continuous Integration and Continuous Development (CI/CD) pipeline using Jenkins to ensure tools can be rapidly deployed, tested, and integrated.