*Spring Geek Trak 2021*

**(May 2-5, 2021)**

# Network Security Monitoring

## Day 1

### ***Section 1: Workshop Overview and Orientation***

Day 1 is used to get everyone signed into LMS. The LMS is used to centrally distribute slides, lab documents and short quizzes for knowledge checks. Day 1 also introduces everyone to the lab environment that they will be using to apply content discussed. Once everyone has verified access, an introductory discussion on Network Security Monitoring starts.

- **Verifying Material Access**
- **Lab Environment Orientation**
- **Introductory Discussion**

## Day 2

### ***Section 2: Splunk***

Day 2 is used to discuss Splunk as a solution for network security monitoring. It starts with a general overview of the solution. Following that, a demo on how to get the solution up and running to start collecting data. Day 2 ends with a hands-on lab to apply lessons learned through the day.

- **Splunk Installation and Usage**

## Day 3

### ***Section 3: Security Onion***

Day 3 is used to discuss Security Onion as a solution for network security monitoring. It starts with a general overview of the solution. Following that, a demo on how to get the solution up and running to start collecting data. Day 3 ends with a hands-on lab to apply lessons learned through the day.

- **Security Onion Installation and Usage**

## Day 4

### ***Section 4: Putting It All Together***

Day 4 is used to bring everything together. It starts with building a simple network environment. Once the simple network environment's functionality is confirmed, the solutions learned during the workshop is applied to it.

- **Applying Tools to a Network Environment**