Peeling Back the Layers and Peering Through the Clouds with Security Onion – Wes Lambert

Thanks for your interest in this workshop! It is hoped that by attending, you'll gain a better grasp for how you can help to improve your organization's posture with regard to cloud security monitoring, or simply learn more about cloud monitoring mechanisms.

Below are the requirements for participation in this workshop. Keep in mind, you do not need to satisfy the below requirements if you don't plan on actively participating -- only if you intend to follow along at home.

AWS

If you would like to follow along at home with setting up Security Onion in AWS, you will need the following:

*Note: While Security Onion itself is completely free, if you require usage of AWS infrastructure for anything other than what qualifies for the free-tier, you will incur charges (albeit minor, in this case). This requires a valid credit card to be associated with your account, and we will be using an instance type (only for the Security Onion instance) that does not qualify for the free tier. Additionally, charges are incurred for usage of the traffic mirroring feature, which we will demonstrate. In all, attendees should expect to spend less than a couple dollars, total.

AWS Account
Sign up for an account: https://aws.amazon.com/free/

Ensure the root user account is locked down using MFA.

Take note of the access key/secret key for your use if planning on participating in automated deployment.

Additional resources:
Connecting to your instance:
https://docs.aws.amazon.com/quickstarts/latest/vmlaunch/step-2-connect-to-instance.html

Follow Along

If you would like to follow along with a text-based version of the instruction, you can consult the steps in the following document.

https://docs.google.com/document/d/1DZsfjOLCGC8F1I4rUO2yltVJksJeYCJGWGZbWQA0TOg/edit?usp=sharing

Automated Deployment

If you would like to follow along at home with setting up Security Onion in AWS in an automated fashion, you will need to have the following set up in advance, with access to the internet:

https://github.com/Security-Onion-Solutions/securityonion-cloud/

VM/Host

Ubuntu 18.04