RSAConference2020

Learning Labs

HUMAN ELEMENT

# Put the Analysis Back in Your SOC!

## Learning Lab Wrap Up

**Kristy Westphal, Instructor**

# Table of Contents

**KEY CONSIDERATIONS** ..... **3**

**LESSONS LEARNED** ..... **3**

**INSTRUCTOR CONTACT INFORMATION** ..... **3**

# Learning Lab Summary

The following is a summary of the Learning Lab Put the Analysis Back in Your SOC!, which was delivered at RSA Conference 2020. Despite automation and orchestration, we still need the human touch and recruiting good analysts in your security operations center is a challenge. The good news is that there is plenty of good talent out there, but they may not have the experience or training that is needed. This session provided a technical path towards teaching new analysts how to confidently assess security events.

## Key Considerations

Teaching analysis is not easy. I took the approach of reading logs as a starting point because I feel like we our analysts get the opportunity to learn the basics before we throw them into roles in our Security Operations Centers. In fact, we almost design the roles any more to not do any analysis. This does a disservice to our employees as they will struggle to grow in our profession if they can't do simple analysis.

Having a program to train others who may want to change careers is also a way to open up the pool of potential employees in a market where it can be a challenge to find talent. Take the material in the slides (logs and slides can be found here: https://drive.google.com/drive/folders/1T25u-5HiDvv2DDmJAOX8HzUIM_3HMh3X) and use them for your own organization and help improve the quality of the services we offer in our Security Operations Centers and other security roles!

## Lessons Learned

- There are many ways to do analysis. Provide options, let the analyst pick the best way for them and encourage them.
- Have your analysts ask questions. Encourage them to challenge theories.
- It's OK for analysts to be ignorant. Just encourage them to come up with hypotheses and then prove them.
- Keep the training going. Don't just do it once and walk away. To keep skills up to date, have analysts learn on an ongoing basis.
- Enlist senior folks to help train the junior folks.

## Instructor Contact Information

Please keep the conversation going! This is truly a community effort as we all learn from each other. You can find me here: kmwestphal@cox.net