Malware Archaeology Training

Mitre ATT&CK, What is it, how to use, and apply it to your organization

- Length: 1-Day training
- Date: Apr 9th, 2018
- Location: HouSecCon

Course Description:

Mitre has created the “Adversarial Tactics, Techniques & Common Knowledge” (ATT&CK) to help security practitioners understand the actual techniques and tactics that adversaries use against us. The advantage of ATT&CK is it allows us to build a framework to understand how we might detect, respond, and prevent many of the tactics. Creating your own ATT&CK framework provides for a way for us to map what technologies, procedures, playbooks, reports/queries, and alerts we have, and then map any gaps that we have that then can be addressed.

This course is intended for any Information Security or IT professional. The focus will be on What ATT&CK is, How to start using it, and resources available to you. We will walk through mapping your technologies and options to self-assess yourself against ATT&CK and how to know if you are ready to defend against these type of adversarial techniques. All attendees will get a copy of LOG-MD Professional as part of the class.

Outline:

- Introductions, Goals & Objectives and Terms & Concepts
- What is ATT&CK
- Resources for ATT&CK
- Malware Management – Where to get the latest techniques and TTPs
- Lunch – Sponsor
- How to use ATT&CK
- Self-Assessment exercises
- Filling in your own ATT&CK Matrix
- Questions and Discussion

Target Audience (Who should take the course)

This course is intended for any Information Security or IT professional, newbs to seasoned pro’s, this class is for everyone.

- Students will need a laptop with Word, PDF and Excel. All class documentation will be provided on a USB drive to each student.