Title: Commanding YARA
Date/Time: (1-Day) Thursday, April 12, 8am-5pm

Description:
YARA is a powerful and free sleuthing tool that belongs in every threat, incident response or SOC team. It runs on any platform, is open source and is small enough to be an easy inclusion to any trusted tool set. Its ability to sift through data, identify files based on logic - not just by simple comparison but also via fuzzy logic - makes YARA pretty unbeatable. It can be used simply for insight on an isolated event or in sophisticated manner as part of an incident response or research laboratory. Those not using YARA are missing out on key intelligence capability. Its ease of use and ability to rapidly deploy means you can get into YARA quickly but can just as easily lead to missing the sophisticated and powerful ways to use it.

Example YARA applications from the class:

- Employ detection fragment strategies to identify the write elements of a file for identification and classification
- Identify files by signature, by structure and organization
- Classify single and groups of file
- Employ logical structures to stack, cluster, and iterate through data in file a for detection or classification.
- Use of negation and inverse detection tricks
- Condition line only detections
- Complex rule usage

Instructor: Monty St. John (@montystjohn)
Monty St John has been in the security world for more than two decades. When he is not responding to incidents he teaches classes in Threat Intelligence, Incident Response and Digital Forensics. Monty is a frequent contributor to community and industry events, presenting at BSides D.C., BSides Austin, Charm, Derbycon and several others. He lives in Austin, Texas and is a security trainer for CyberDefenses, Inc. based out of Round Rock, Texas.

Course Outline:
- Introduction
- Setup
- YARA fundamentals
    - Lab 0 - YARA introduction
    - Strategies (direct, indirect, inverse)
    - Logic (Declarative, Connective, Cause & Effect)
    - Lab 1 - strings, hex & regex
- File Magic
    - File types and file magic
    - Lab 2 - file magic (PE, PDF, Zip)
- Structure and Format
    - Files and data organization
    - Lab 3 - Email (a & b)

- Data and Content
    - BOF & EOF
    - Lab 4 - B/EOF (PDF, JPG)
- Structural Detection
    - Lab 5 - Detection by Format (PDF)
- YARA Keywords
    - Keywords
    - Rule organization basics
    - Lab 6 - Keyword modifications (PE/malware)
    - Lab (a-c) - Hex Jumps & Regexes (PE/malware)
- Global Rules & Organization
    - Lab 7 - Classifying Emails
    - Negative Space (inverse matching) topic
    - Lab 7a - Inverse matching email
    - Detection strategy & logic (one more time)
    - Classifying Malware Families
    - Core identification
    - Lab 8 - Malware Classification (core)
- Variations and derivatives
    - Lab 9 - Malware Family Classification
- YARA in Action
    - Lab 10-12 - Interrogate a file and use YARA to provide boilerplate for reporting.
    - Lab 13-16 - Dissect a file to understand its functions, composition, communication and protections.

Who Should Attend:

- Individuals new to or desiring a better understanding of how to use YARA.
- Professionals who deal with technical issues but feel they do not have enough background in using YARA successfully.
- Technical professionals that need to be armed with greater knowledge of incident response, threat Intelligence and their role in resolving incidents.

Student Requirements (what should they bring with them)

- Laptop required
- Basic knowledge of computers, technology and command line interface (CLI)
- Ability to open and operate browsers, find and use the command line, execute scripts and open programs
- Requires knowledge of Linux
- No prior knowledge of YARA required
- Understanding of virtual machines (VM) and how to use one