Title: Intro to Threat Intelligence
Date/Time: (1-Day) Wednesday, April 11, 8am-5pm

Description:
Defining Threat Intelligence (TI) in an understandable way can be frustrating. Every cybersecurity vendor and expert seems to have their own definition of what it entails, not to mention just as numerous a number of procedural viewpoints to go along with it. One method to keep the concept of TI clear is to describe its actions with verbs, such as “collect”, “detect”, “investigate”, “analyze”, “alert”, and “report”. If you use those key words as pivots, it’s easy to enumerate the functions of TI. An example of a few would be:

- Identify and collect threat and high-value information (**collect, analyze**)
- Determine the impact of events and incidents (**analyze, investigate, report**)
- Create and present threat briefings (**alert, report**)
- Correlate observed threats and associated adversary profiles to activities, current events and incidents (**analyze, investigate, detect**)
- Leverage tradecraft and experience to identify threats and suggest security measures to mitigate risk and inform decision making (**analyze, investigate, detect**)

The list continues on. Any pivot around these keywords are likely aspects of the diverse portfolio of intelligence tradecraft. While not included in keyword list above, two other elements to consider are “data” and “transformation”. Threat Intelligence is only as good as the data that feeds it and the transformation that changes that data into something useful. All eight require a clear strategy to be effective, to prevent and predict future threats while better defending against present ones.

The course contains 12 labs to intensify a student’s introduction to TI. The course begins with a discussion of key concepts and principles and then builds to convey an understanding of how it fits in your company and when, where and how to use it. The labs assist those aspiring to understand TI lock down when and where it plays a role and how.

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
- Key Concepts & Principles
    - The Threat
    - The Attribution
    - The Resources
    - Modeling Threat Intelligence
        - Strategic Intelligence
        - Operational Intelligence

        - Tactical Intelligence
- Intelligence Driven Strategy
- Temporal Aspects
- Use Cases & Benefits
- Home Advantage
- Role in Network Defense
- Intelligence Cycle
    - Planning
    - Collection
    - Transformation
    - Analysis
    - Reporting
- Application and Integration
- Storage and Dissemination
- Managing the Program
- Wrap up and Close

Who Should Attend:

- Individuals new to threat intelligence but with a need to understand its fundamentals
- Professionals who deal with technical issues but feel they do not have enough background in threat intelligence and its use
- Technical professionals that need to be armed with greater knowledge of incident response, threat intelligence and the role it plays

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
- Prior threat intelligence experience not required
- Understanding of virtual machines (VM) and how to use one