ATX-Y-1 -YARA

Yet Another Regex Analyzer or YARA is a simple and highly effective way to identify, classify, and categorize files. While most often employed in the context of malicious files, YARA is not limited in that regard and can be directed at **any type** of file. This ability makes it a valuable sleuthing tool in your arsenal identify, understand and ultimately prevent unwanted influences.

ATX-Y-1 - YARA will help you:

- Identify, classify, categorize and analyze and then leverage file-derived intelligence to detect and respond to threats
- Piece together adversary campaigns and threat activities
- Transform unknown/unwanted files into a well of usable intelligence
- Enrich existing intelligence to analyze, understand and profile adversaries and their tactics, techniques, tools, and procedures

We are barraged by files, from the unwanted to the expected. By email, FTP, web browser download, chat program transfers and hundreds of other ways, files enter our environment and present a challenge to security. We employ an equally labyrinthe amount of tools in response to identify the expected and benign while sequestering the malicious and unwanted. In most cases we succeed. When we fail, what follows is an expensive and time-intensive post mortem to find out why, what happened, and how it affected us. In both these areas YARA shines. Its ability to identify and organize files assists in the latter and enhances understanding in the former. This kind of file insight transforms into threat intelligence that can help you understand how a group of individuals in your organization came to be targeted by a phishing campaign or detect the same or similar patterns of file activity on systems across your network.

Regardless of your use of YARA, the need for critical intelligence to combat and understand how adversaries operate couldn't be higher. ATX-Y-1 YARA course will teach you and your team how to find, refine and leverage that intelligence.

Module 1 - The Basics
Topics: Course Introduction, Syntax, YARA Setup, Variable Use, Matching, Negative Matching, Inverse Matching
Module 2 - Advanced Concepts
Topics: Detection Concepts, Rule Organization, Pattern/Logic Matching, Classifying, Categorizing
Module 3 - Tools and Efficiency
Topics: YARA Tools, Do's and Don'ts, Enhancing Scanning Speed, Large Volume Scanning, Network Scanning