Incident Coordinator Track Overview

The Incident Coordinator track is part of a multi-track training program created by Tracer FIRE staff to indoctrinate participants to the overall methods that a high performing CSIRT (Cyber Security Incident Response Team) uses in its daily mission of hunting for and tracking down of attackers operating on the corporate enterprise network. The primary mission of CSIRTs is to continually patrol their organizations enterprise networks and systems in order to detect malicious activity and remediate these attacks. This is a complex and demanding job so it's not for the faint of heart.

In this track, attendees will be provided with a perspective on how effective CSIRTs are established and how they coordinate with other groups within their organization to maximize their effectiveness. In addition, this track will include discussions on the various internal and external groups an Incident Coordinator will have to interface with to ensure a smooth, effective response to a severe incident; while also ensuring their team can properly perform response activities. Finally, we will discuss the role of the Incident Coordinator in maintaining a "Big Picture" view to understand the event as a whole, and avoid being distracted by noisy, obvious attacks, allowing an adversary to conduct quieter attacks without being detected.

These topics are utilized in the exercise portion of the training to ensure the team performs well on the challenges presented, and that technical information gained from various artifacts are shared throughout the team. Also, having an Incident Coordinator will be vital in piecing together the clues scattered throughout the challenges which, when combined, will provide insight into the nature of the adversary, the activities they are conducting (and why), and bring everything together to create a coherent narrative of what has happened.

The topics covered in this track include:

- Creating a CSIRT
- The Role of an Incident Coordinator
- Response Priorities
- Delegating Authority
- Dealing with a Crisis (Crisis Mode!)
- Asking for Assistance
- Reporting to Executive Management

Recommended Reading:

- Former PNNL CIO Jerry Johnson, Interview with John Foley of Information Week, "7 Lessons: Surviving A Zero-Day Attack", September 19, 2011. http://www.informationweek.com/news/security/attacks/231601692

- Ben Sapiro, Liquid Matrix, “We Are Losing”, February 21, 2012, http://www.liquidmatrix.org/blog/2012/02/21/we-are-losing/
- Carnegie Mellon Software Engineering Institute, “Handbook for Computer Security Incident Response Teams (CSIRTs)”, April 2003. http://www.sei.cmu.edu/reports/03hb002.pdf