Workshop : Adversary Hunting, Detection and Compromise Assessment

Organizations are always under attack and
adversaries of all skill levels are on the lookout for new vulnerabilities, tools, and techniques to compromise an enterprise network. It becomes really difficult as well as important for defenders to stay on top of the game. The workshop is intended towards people interested in learning the methodology and approach for hunting, detection and compromise assessment in an enterprise environment.

Target Audience: People interested or working in Security Operation Centre, Blue Team, Incident Response, Threat Hunting or any defensive role in their organizations.

High Level Course Description:

- Introduction to Adversarial Detection & Hunting
- Tools, Techniques, and Procedures to find bad apples in your enterprise environment
- Overview of MITRE ATT&CK Methodology
- Data Collection in Enterprise Networks
- Developing Hypothesis for Detection and Hunting
- Common Indicators of Compromise
- Setting up open source Compromise Assessment environment
- Setting up Open Source Deception
- Detecting and Hunting for common attack and post-attack scenarios in an enterprise network
- The role of effective threat intelligence in Detection and Hunting
- Wrap up

Hardware/Software Requirement:

- 25+ GB free hard disk space
- 4+ GB RAM
- VMware Player/Fusion/Workstation installed on base machine
- External USB allowed
- Administrative access on the system