Information Security and Incident Management

Course Contents:

Module 1: Introduction

• Brief introduction to the incident management process. It is expected that the audience has a generally good understanding of the overall incident management process. Participants are expected to be well-versed with the broad understanding of security controls such as firewalls, intrusion detection systems, security incident and event management systems, etc.

Module 2: At tacks Against Web & SSH Servers

• This module covers alerts related to accepted inbound port scans or aggressive SSH connections. You are tasked with carrying out the investigation from scratch. The target server is a website that runs either on Apache or on IIS. You are required to understand the log formats, parse the logs using a tool of your choice, request for live forensics data of the server, and develop your hypothesis.

• Tools/Technologies covered: SSH server logs, web server logs, Unix utils etc.

Module 3: Advanced Persistent Threats

• This module dives straight into an advanced threat detected within your organization. You are given the symptoms of the attack, and then are required to investigate the incident using an actual network setup for this purpose. You are provided with logs that you request based on the hypothesis you are building along with access to endpoints for live forensics.

• Tools/Technologies covered: Web proxy logs, Active Directory, Windows endpoint, antivirus, Sysinternals Suite etc.

Module 4: Data Leakage

• You have been informed by a particular manager within the marketing department that there is a suspicion of a user or particular set of users leaking out customer data to the competition. You are required to investigate this discreetly.

• Technologies covered: DLP logs, proxy logs, endpoint, Active Directory, etc.

Module 5: Ransomware Infection

• Your systems are being impacted with ransomware. Your anti-virus is unable to protect your endpoints, and the infection may begin spreading rapidly. You need to investigate this ransomware quickly and understand how it spreads.

• Tools/Technologies covered: Ransomware samples, malware analysis, reverse engineering, Cuckoo sandbox, etc.

Module 6: Payment System Compromised

• You have received notification from your Fraud Control Unit that some counterparties have informed them of a potential breach on the SWIFT payment system. You are required to undertake the investigation end to end and determine the source of the leakage and also carry out a root-cause analysis.

• Technologies covered: Unix system logs, Windows system logs, application logs