INCIDENT RESPONSE AND THREAT HUNTING

- 5 Days Programme
- 40 CPE's
- Laptop Required

Who is this Course for?

This course is specially designed for Cyber Security professionals who like to enhance their career by specializing in Threat Hunting and Incident response process. This is an in-depth hands-on course designed especially for Threat hunters, Incident responders, SOC Analysts and it will give them an understanding about the various advanced threats that can target/exists in an organization and how to detect and remediate those threats.

This course covers the importance of communication during a cybersecurity incident response effort, analysing the symptoms of an incident in progress, the use of forensic tools, and the incident recovery and post-recovery processes. Completing this course, will help you prepare to become a Cybersecurity Analyst and ensure that your organization is properly insulated from risk.

Course Introduction

Imagine yourself in this scenario. You are an Incident responder working for one of the big Banks. Your job is to detect threats as fast as possible and once they are detected, remediate them quickly to avoid further damage. You received an update from your Threat Intel group that there might be some potential state sponsored threat actor targeting your organization. Your job now is to find out if your organization has been breached and if yes, how many assets have been compromised. Has the threat actor been successful in taking out sensitive data from your organization? This is a very challenging scenario as these threats can always exists in your organization without anyone's knowledge. You need to have access to the right processes and tools to be able to successfully hunt for these threat actors and take the necessary actions to contain the assets that were affected by this threat. This course will teach you the modern processes as well as tools available for Threat Hunting so that you are in a better position to handle these scenarios. At the end of this course, you'll have a greater understanding of the threats that affect private, corporate, and government networks, and the knowledge to prevent attacks and defeat them.

Course Objectives

This advanced level course will teach the attendees to:

- Accurately identify Compromised and Affected Endpoints
- Understand the importance of Continuous Threat Hunting
- Perform Triage assessments and find out any potential symptoms of Data leakage and loss of system integrity.
- Learn how to Detect, Contain and Remediate incidents.
- Leverage Cyber Threat Intelligence in the Incident Response and Threat Hunting process.

DETAILED COURSE DESCRIPTION

DAY 1-Threat Hunting Introduction

- Incident Response and Threat Hunting Concepts
- Understanding Current Threat Landscape and Attack Life Cycle/Attack Kill Chain
- Threat Hunting Vs Incident Response
- Malware analysis fundamentals
- Various approaches to malware analysis
- Static and Dynamic Analysis
- Steps in Threat Hunting Process
- Leveraging Bro logs for Threat Hunting
- Different Tools available for Threat Hunting
- Threat Hunting in AWS and Azure
- Leveraging Cyber Threat Intelligence for performing Threat Hunting
- Performing live forensics and Threat Hunting by using Google Rapid Response.
- Triage and Endpoint Detection and Response using Google Rapid Response.

DAY 2- Memory Forensics

- Memory forensics fundamentals
- Memory Acquisition and Examination
- Memory Analysis Timeline Creation
- Identifying Rogue processes, Process DLLs and Handles in memory.
- Reviewing Network Artefacts, evidence of code injection, Check for the signs of Root kits, malwares, acquiring Suspicious processes and drivers.
- Advanced Memory Analysis with Volatility.
- Leveraging Volatility to analyze real sample malwares such as Stuxnet, Conficker, BlackEnergy etc.
- Leveraging results/IOC's from memory forensics/ analysis for performing Threat Hunting
- Introducing Redline for doing Memory Analysis
- Using Redline for Auditing and Collecting all running processes and drivers from Memory, File System Metadata, Registry data, event logs, network information, services, tasks and web history.
- Leveraging Redline for creating Memory timeline
- Running yara rules against memory image
- Volatility Lab

DAY 3- Detecting and Analysing Intrusions through Disk Analysis

- Mounting raw disk file in Windows/Linux
- Understanding Application compatibility Cache, Prefetch, Shimcache, Amcache, RecentFileCache
- Analysing Windows Volume Shadows
- Detecting Lateral Movements
- Identifying Malware Persistence
- Adversary Tactics, Techniques, and Procedures (TTPs)
- Analysing windows event logs
- Leveraging Autopsy (Sleuth kit) to examine raw disk
- Filesystem Timeline Creation and Analysis
- Gathering and Analysing artefacts from Registry, file system, prefetch, Browser cache, Browser history, Windows event logs stored in raw disk image
- Using Regripper tool to analyze specific content in the registry.
- Exporting registry Artefacts from Autopsy and analysing them selectively in the Windows Registry Recovery or WRR tool.
- Super-timeline Creation, Analysis and Examination

WHO SHOULD ATTEND

- Incident Response Team Members
- Threat Hunters
- SOC Analyst
- Experienced Digital Forensic Analysts
- Information Security Professionals
- Federal Agents and Law Enforcement Personnel
- Red Team Members
- Penetration Testers
- Exploit Developers

DAY 4- Threat Hunting and Anti-forensics Detection

- Incident response in real world
- Threat Intelligence Creation and Use During Incident Response and Threat Hunting
- Introducing Cuckoo Sandbox and using it for understanding Malware behaviour
- Leveraging Mandiant IOC Editor to create IOC's.
- Static Analysis Tools
- Detecting Packets and Protectors
- Strings extraction and analysis
- PE structure and headers analysis Import table analysis
- Process Explorer and Process Monitor Analysis
- Dynamic Analysis Tools
- Malware and Anti-Forensic Detection
- Anti-Forensic Detection Methodologies

DAY 5- Threat Hunting Final Lab

In this lab you will be presented with a live scenario and you will be asked to build a timeline by combining all the knowledge that you have gathered in the last few days. This include Memory analysis, Disk Analysis, Prefetch Analysis, Network Artefacts Analysis, Registry analysis, Process analysis. This lab can take anytime from half a day to complete full day depending on how fast you can discover artefacts and collect evidences.

Technical Pre-Requisites

- Attendees should have good knowledge of Networking and TCP/IP concepts, basic network troubleshooting, Basic level of Knowledge of VMware workstation such as setting up Guest OS, VMware networking.
- The attendees should have some background in network traffic analysis, log analysis or Security Architecture and system administration.
- They must have a working knowledge of windows operating system, file system, registry and use of the command line. Familiarity with Active Directory and basic Windows security controls, plus common network protocols, is beneficial.

Laptop Requirements

- CPU: 64-bit Intel i5/i7 - x64 bit 2.0+ GHz processor or more
- 16 GB RAM or greater, 200 GB of Hard Disk Drive
- VMWare fusion/workstation or VMware Workstation player.
- 64-bit version of Windows 7(or above) or Mac OSX
- Install 7-zip on your host OS
- Disable credential guard
- Admin level access to the host operating system as well as guest operating system.
- Wireless 802.11 compatibility