A tesserent Company

# CYBERSEC FIRST RESPONDER™

## DURATION: 2 DAYS

CYBER SECURITY

The CyberSec First Responder™ Certificate Course is designed to equip the organisation's IT staff members with the capability and knowledge to be able to respond to an incident in an effective and timely manner. Knowing how to act promptly during an incident can significantly reduce the incident's negative impact and ensure that an incident response investigation can be performed without delay.

The two-day training is a technical and hands on workshop that will introduce attendees to various open source and free tools that can be used to capture and analyse artifacts that are critical during an incident investigation.

## WHO SHOULD ATTEND

**This course is intended for:**

- Technical staff members who are tasked to first respond to cyber security incidents. Typical roles include: Systems Engineer, Systems Administrator, Systems Analyst, Network Engineer, Network Administrator, Network Analyst, Helpdesk Level 1 & 2, Security Analyst, Threat Analyst, Infrastructure Manager, IT Manager
- Anyone involved in Governance or Risk and who needs to gain a better understanding of how an attacker thinks

## LEARNING OUTCOMES

**This course is designed to:**

- Ensure that staff members who are on the front lines of responding to incidents as they occur are well equipped to perform this critical role
- Provide front line staff members the knowledge on how to satisfactorily collect forensic evidence.

## COURSE CONTENTS

### PHASE 1: INTRODUCTION TO INCIDENT RESPONSE

- Common pitfalls
- Common pain points that organisation make with regards to incidents
- Prevalent threats/attacks
- Who are the threat actors
- What are the most common attack that are currently used
- What is an incident and how to prepare for it
- Incident life cycle
- Regulatory bodies and Law
- Evidence handling best practices
- Chain of custody discussion
- Forensics go kit
- War stories and scenarios
- Sharing of war stories and their root cause
- What could have been done better to prevent the incident

### PHASE 2: HOW HACKERS DO IT

- Introduction to malwares
- Type of malwares
- Common protection against malwares
- Common attack techniques and lifecycle
- Common attacker behaviour
- Typical attack lifecycle

### PHASE 3: DATA COLLECTION (DEMO / HANDS ON)

- Disk image gathering
- Introduction to tools used for disk image creation
- Demo and hands on workshop on creating disk images
- Memory image gathering
- Introduction to tools used for memory dump collection
- Demo and hands on workshop on memory dump collection

### PHASE 4: INTRODUCTION TO FORENSIC ANALYSIS

- Autopsy 101
- Introduction to forensic analysis tools
- Demo and hands on workshop on using the tool called Autopsy
- Basics of memory forensics
- Introduction to memory forensics analysis tools
- Demo and hands on workshop on using memory analysis tools

### PHASE 5: CLOUD IR

- Triaging incidents in the cloud
- Conducting M365 incident response

### PHASE 6: GOOGLE-FU (OPTIONAL, IF TIME PERMITS)

- Using Open Source Intelligence (OSINT) in incident investigation
- How can public data be used during an incident investigation

CYBER SECURITY
**WE HAVE YOU COVERED**

**1300 767 592**
**customerservice@alc-group.com**
**alctraining.com.au**

ALC.Training
@alcgroup
alc-training