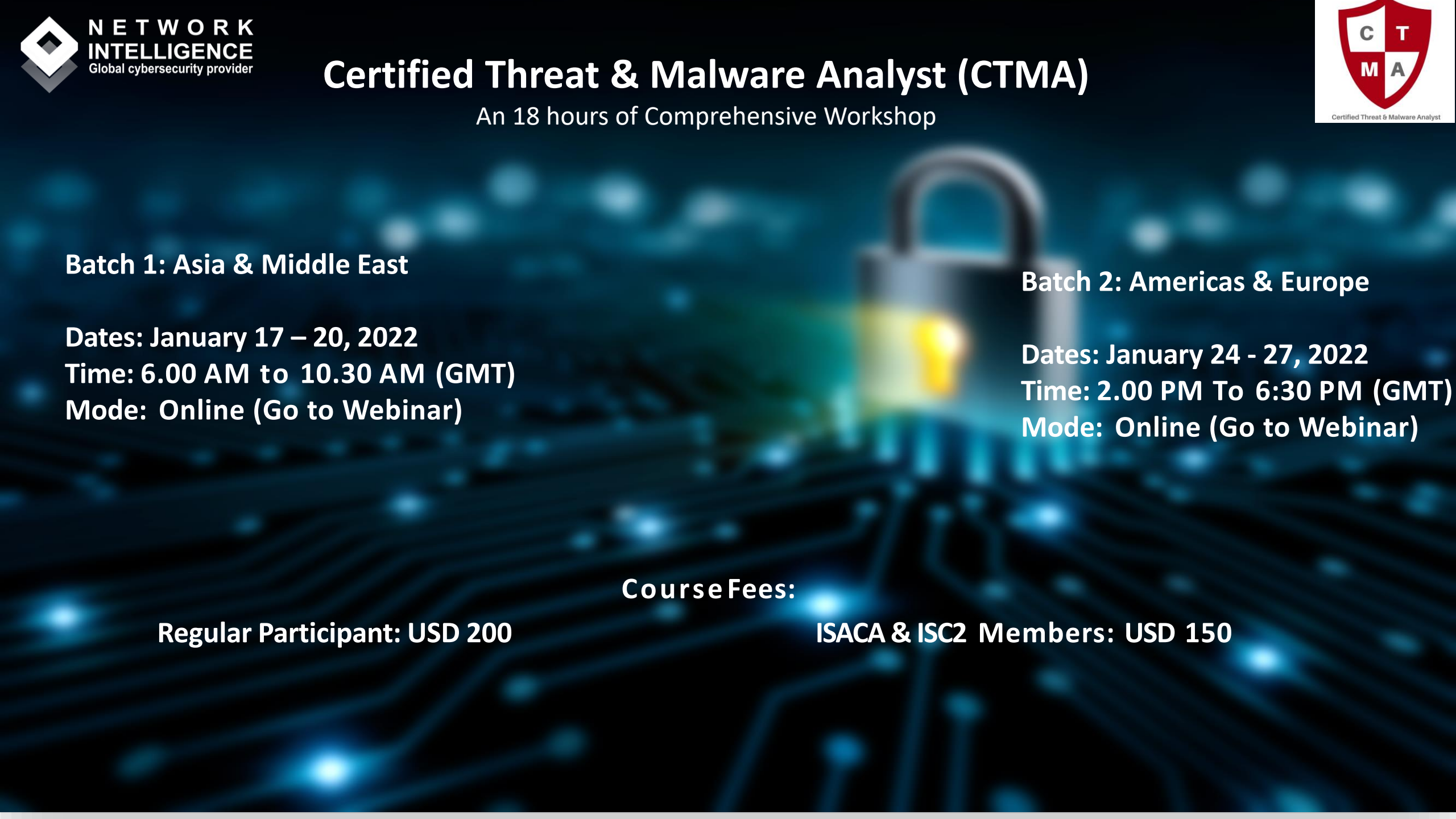
NETWORK INTELLIGENCE
Global cybersecurity provider

Certified Threat & Malware Analyst (CTMA)

An 18 hours of Comprehensive Workshop



Batch 1: Asia & Middle East

Dates: January 17 – 20, 2022
Time: 6.00 AM to 10.30 AM (GMT)
Mode: Online (Go to Webinar)

Batch 2: Americas & Europe

Dates: January 24 - 27, 2022
Time: 2.00 PM To 6:30 PM (GMT)
Mode: Online (Go to Webinar)

Course Fees:

Regular Participant: USD 200

ISACA & ISC2 Members: USD 150

NETWORK INTELLIGENCE
Global cybersecurity provider

CERTIFIED THREAT & MALWARE ANALYST (CTMA)

Introduction:

For defenders to become more relevant in disrupting the kill-chain, it is imperative that they also rapidly evolve their detection strategies.

No longer are static rule-based detections or simple keyword searches going to help SOC teams to identify advance threats in their environments.

A more proactive approach is the need of the hour.

The CTMA training is focused on a coverage of both Malware Analysis and Threat Hunting. It is designed to ensure that all aspects have a real-life scenario-based approach explaining the core steps needed to perform either Malware Analysis or Threat Hunting

C T M A
Certified Threat & Malware Analyst

OBJECTIVE OF THE CTMA CERTIFICATION PROGRAM

Objectives

- How should one analyse a file to determine if it is malicious or not?
- What tools can be used in Static and Behavioural Malware Analysis?
- How should hunts be carried out?

Who Should Attend?

- Chief Security Officers (CSO), Chief Technology Officers (CTO), Chief Information Officers (CIO)
- SOC Experts & Analyst.
- Security practitioners and managers.
- Anyone interested in starting out in Malware Analysis & Threat Hunting.

“Remember….. you are the Centre of Security”

NETWORK INTELLIGENCE
Global cybersecurity provider

Course Content

Certified Threat & Malware Analyst

Session 1: Introduction to Threat Hunting

- Need for Threat Hunting
- Threat Hunting Framework
- Typical Data Sources
- Threat Hunting Maturity Model
- What is a Threat Hunter?
- Threat Hunting Skills
- MITRE ATT&CK
- MITRE CAR
- Current Attacks Case Studies

Session 2: Practical Threat Hunting

- Types of Threat Hunting
- Analysis Techniques used by a Threat Hunter
- Creating Hypothesis
- Understanding Log Sources in an Organisation
  - Network
  - OS
  - Solutions
- Hunting on Network log sources
  - Firewall
  - DNS
- Hunting on OS log Sources
  - Windows
  - Linux
- Threat Intelligence:
  - Threat Intelligence Feeds
  - Operationalizing Threat Intelligence
- Metrics for Threat Hunting Success
- Reporting for Threat Hunting

"Remember….. you are the Centre of Security"

NETWORK INTELLIGENCE
Global cybersecurity provider

Course Content

Certified Threat & Malware Analyst

Session 3: Introduction to Malware Analysis

- Types of Malwares
- Skills required by a Malware Analyst
- Levels of Malware Analysis
- Sandboxing
  - Online sandboxing
  - Setting up a malware analysis lab
    - Procedures
    - Tools required
- Non malicious vs malicious behaviour
- Malware attack case studies

Session 4: Practical Malware Analysis

- Static Analysis of Malware:
  - Files and File Formats
  - Properties of files
  - Content of files
  - Malware Funnelling
- Behavioural Analysis:
  - Analysing Process Behaviour
  - System Activity monitoring
  - Analysing network communication and packet captures
- Extracting IOCs to be used for Blocking
- Anti-Analysis techniques of malware
- Analysis of trending malwares

“Remember….. you are the Centre of Security”

NETWORK INTELLIGENCE
Global cybersecurity provider

Certified Threat & Malware Analyst

Trainer Details

Mufaddal Taskin,
Lead Trainer
Network Intelligence

Mufaddal has over 26 years of diverse experience in technology solutions. His technical abilities span across Malware Analysis, Threat Hunting, Networks, Web Apps, Digital Forensics & Incident Response, Penetration Testing, SOC and ISO standards Compliance. Mufaddal has created custom course outlines as well as conducted the same for a variety of high technologies clients of Network Intelligence

Lionel Faleiro,
Practice Lead – Digital Forensics & Incident Response
Network Intelligence

Lionel is passionate about training and working in DFIR. He comes with an experience of 10 years in IT and Cybersecurity. He began as a SysAdmin then a Security Trainer and now leads the Digital Forensic Practice and Incident Response division at the firm. He has technical hands-on with Malware Analysis, Threat Hunting, Compromise Assessment. He has solved numerous cases during his tenure at Network Intelligence and is an avid gamer and street photographer as well.

Registration form : https://forms.office.com/r/icZmPcvfp5