SYLLABUS

CYBER SECURITY · COURSE HANDOUT 2026

MALWARE ANALYSIS

TIC . DYNAMIC . BEHAVIOUR
SANDBOXING . DEBUGGING
CATORS . DETECTION . REPO

DURATION	LEVEL	MODULES	MODE
50 Hours	**Advanced**	**8**	**Classroom · Online · Hybrid**

01 COURSE OVERVIEW

A malware analysis course from safe sample handling to behavioural and code-level analysis. The course builds an isolated analysis lab, then works through static triage, dynamic execution monitoring, unpacking, assembly-level review and indicator extraction, using real but defanged samples.

Learners produce analysis reports with detection signatures for each sample studied.

WHO IT IS FOR

- SOC and incident response analysts
- Threat intelligence teams
- Reverse engineering enthusiasts
- Security researchers

PREREQUISITES

Operating system internals, networking, and comfort with Windows administration. Assembly exposure is helpful.

02 LEARNING OUTCOMES

01 Build and isolate a malware analysis lab safely.

02 Triage samples with static indicators and hashing.

03 Observe behaviour with process, file and network monitoring.

04 Identify packing and unpack simple samples.

05 Read assembly to understand key routines.

06 Extract host and network indicators of compromise.

07 Write YARA rules and an analysis report.

03 MODULE STRUCTURE

8 MODULES

01 LAB AND SAFETY

- Isolation
- Sample handling
- Analysis workflow
- Snapshots
- Legal and ethical rules

02 MALWARE TYPES

- Trojans
- Loaders
- Rootkits
- Ransomware
- Info stealers
- Living-off-the-land techniques

03 STATIC ANALYSIS

- File headers
- Strings
- Entropy
- PE structure
- Imports and exports
- Hashing and reputation

TOOLS

PESTUDIO · CFF EXPLORER

04 DYNAMIC ANALYSIS

- Process monitoring
- Network capture
- Sandbox reports
- File and registry changes
- API calls

TOOLS

PROCMON · WIRESHARK · CUCKOO

05 PACKING AND OBFUSCATION

- Packers
- Anti-analysis tricks
- Shellcode basics
- Manual unpacking
- Script deobfuscation

06 CODE ANALYSIS

- x86 essentials
- Control flow
- Key routine identification
- Disassembly
- Debugging

TOOLS

GHIDRA · X64DBG

07 DOCUMENT AND SCRIPT MALWARE

- Macro analysis
- PowerShell and JScript
- PDF objects
- LNK and archive lures

LAB

PHISHING ATTACHMENT ANALYSIS

08 DETECTION AND REPORTING

- IOC extraction
- Sigma rules
- Report structure
- YARA rules
- Threat classification

PROJECT

SAMPLE ANALYSIS REPORT WITH SIGNATURES

04 ASSESSMENT & CERTIFICATION

Module assignments and labs	**25%**
Mini projects	**20%**
Internal assessments	**15%**
Final project and review	**40%**

CERTIFICATION

Learners who complete all modules, submit the final project and clear the review receive a course completion certificate from Kaizen Infinities Private Limited. Project work is documented for the learner's portfolio, and interview preparation is included in the closing sessions.

05 CAREER OUTCOMES

ROLES THIS PROGRAMME PREPARES FOR

MALWARE ANALYST · THREAT RESEARCHER · REVERSE ENGINEER · INCIDENT RESPONSE ENGINEER · DETECTION ENGINEER

CALL US
+91 73051 33996

EMAIL US
apply@kaizeninfinities.com

VISIT OUR WEBSITE
www.kaizeninfinities.com