WINDOWS BLUE TEAMING 2026

Threat Analysis and Detection for SOC and IR Professionals

20–23 July 2026 | Parkroyal Collection Kuala Lumpur

The Windows Threat Analyst Training is an intensive, hands-on program designed to equip cybersecurity professionals with the knowledge and skills to analyze, detect, and respond to advanced cyber threats targeting Windows environments. The session provides in-depth coverage of malware analysis, attack simulations, threat intelligence, and modern detection techniques using industry-standard tools.

Participants will learn how to investigate real-world cyber threats, understand attack methodologies used by Advanced Persistent Threats (APTs), and apply detection engineering techniques to enhance enterprise security. By the end of the course, attendees will be proficient in analyzing malware behavior, detecting malicious activities, and leveraging tools like EDRs, SIEMs, and forensic utilities to strengthen organizational defenses.

Course Trainers:

Abhijit Mohanta is the Co-founder & CTO for Intelliroot with over 17 years of experience in the anti-malware industry. He has several patents, blogs and has presented in well-known security conferences. He has worked in Malware Research labs of well-known organizations, which includes Mcafee, Symantec and Juniper Networks. Abhijit specializes in the area of Reverse Engineering, Malware Detection, Vulnerability and Exploit Research. He co-authored the highly rated book “Malware Analysis & Detection Engineering”.

Madhukar Raina is a Security Researcher with 9 years of experience in information security and trainings. He works for Hack The Box, where he contributes to the malware analysis, reverse engineering, and detection engineering related content and labs. He has previously worked for Zscaler & Securonix as a Security Researcher and Threat Hunter, mainly focusing on malware analysis, reverse engineering deception, threat hunting operations, and adversarial research.

Key Learning Areas:

- **Lab Setup** - Configuring virtual machines, installing analysis tools, and deploying honeypots, Malware Analysis Lab Setup
- **Cyber Attack Frameworks** - Understanding MITRE ATT&CK, Cyber Kill Chain, and threat actor tactics.
- **Threat Intelligence & Hunting** - Identifying attack signals, OSINT research, and dark web intelligence.
- **Detection Engineering** - Writing YARA, Sigma and behavior-based rules APT Techniques & Attack Simulations - Analysis of real-world threats like Mimikatz, Pass-the-Hash and Process Hollowing.
- **Malware analysis** - Teaches to analyse Windows Malwares. (Note: Reverse Engineering is limited here)
- **DFIR & Memory Forensics** - Investigating ransomware attacks, persistence mechanisms, and rootkits.

Organised by: THOMVELL international

Partnered by: Intelliroot SECURITY SIMPLIFIED