

- **Reverse engineering 101**
 - Malware Analysis Primer
 - Basic Static Techniques
 - Malware Analysis in Virtual Machines
 - Basic Dynamic Analysis
- **Advanced Static Analysis**
 - X86 Disassembly Crash Course
 - IDA Pro
 - Recognizing C Code Constructs in Assembly
 - Analyzing Malicious Windows Programs
- **Advanced Dynamic Analysis**
 - Debugging
 - OllyDbg
 - Kernel Debugging with WinDbg
- **Malware Functionality**
 - Malware Behavior
 - Covert Malware Launching
 - Data Encoding
 - Malware-Focused Network Signatures
- **Anti-Reverse-Engineering**
 - Anti-Disassembly
 - Anti-Debugging
 - Anti-Virtual Machine Techniques
 - Packers and Unpacking
- **Incident Response - Preparation & Detection**
 - Real-world incidents
 - IR Management handbook
 - Preparation
 - Investigations
 - Scoping
 - Collecting facts
 - Building an Attack Timeline
 - Setting expectations with Management
- **Incident Response - Data Collection & Analysis**
 - Collection best practices

- Forensic duplication
- Network evidence
- Enterprise services
- Analysis Methodology
- Malware Triage
- Report writing

- **Incident Response - Remediation**
 - Concepts
 - Common mistakes
 - Remediation case study

