COURSE TABLE OF CONTENTS

Velociraptor Endpoint Forensics

OEM: Open Source • Duration: 4 Days (30 hrs)

COURSE MODULES & TOPICS

Module 1: DFIR Foundations and Endpoint Investigation

- DFIR fundamentals
- Endpoint investigation lifecycle
- Evidence-handling principles
- Common endpoint data sources
- Forensic artifacts overview
- Introduction to Velociraptor

Module 2: Velociraptor Architecture and Deployment

- Velociraptor architecture and components
- Deployment models and planning
- Server installation and configuration
- Client deployment and management
- Certificates and communications
- Access control and security hardening
- Operational administration and troubleshooting

Module 3: VQL Fundamentals and Artifact Management

- VQL syntax and query structure
- Data types, plugins, and functions
- Running and interpreting queries
- Using built-in artifacts
- Artifact parameters
- Custom VQL query creation
- Testing and modifying queries
- Hands-on VQL investigation

Module 4: Windows and Linux Endpoint Forensic Collection

- Windows artifact collection and analysis
- Linux artifact collection and analysis
- Process, service, and user investigation
- Windows Registry and event logs
- File-system metadata and hash analysis
- Browser and command history artifacts
- Persistence and scheduled execution
- Evidence collection planning

Module 5: Threat Hunting and Incident Investigation

- Threat-hunting methodology
- Hypothesis development
- Creating and launching hunts

© Koenig Solutions

- Identifying suspicious processes and activity
- Investigating persistence mechanisms
- Searching for IOCs
- Incident scoping across endpoints
- Triage and investigation workflow
- Practical threat-hunting scenarios

Module 6: Advanced Analysis, Automation, and Evidence Correlation

- Timeline-oriented investigation
- Event correlation
- Combining endpoint artifacts
- Custom artifact development
- Reusable collection workflows
- Automating collection and analysis
- Exporting and organizing evidence
- Validation and forensic quality

Module 7: Capstone DFIR Investigation and Reporting

- Simulated endpoint incident investigation
- Evidence collection planning and execution
- Artifact analysis and suspicious activity identification
- Correlating findings and incident assessment
- Documenting methodology and evidence
- Preparing investigation reports