COURSE TABLE OF CONTENTS

Security Operations 7.6 Architect

OEM: Fortinet • Duration: 3 Days (24 hrs) • Code: FCSS-SOC-NSE7

COURSE MODULES & TOPICS

Section 1: SOC Concepts and Frameworks

- Examine security incidents and pinpoint adversary behaviors
- Clarify Fortinet SOC enterprise architecture
- Recognize attack vectors

Section 2: Detection Capabilities

- Set up FortiSIEM incident rules
- Develop queries for searching event logs in FortiSIEM
- Review FortiSIEM incidents

Section 3: SOAR Incident Handling and Threat Hunting

- Examine threat hunting processes and data
- Oversee FortiSOAR incidents
- Establish queues and shifts for workload distribution
- Leverage war rooms for incident handling

Section 4: SOAR Playbook Development

- Set up FortiSOAR playbooks
- Set up FortiSOAR connectors
- Apply Jinja filters for data manipulation
- Identify and resolve FortiSOAR playbook issues