COURSE TABLE OF CONTENTS

FortiSIEM 7.4 Analyst

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

COURSE MODULES & TOPICS

Section 1: Analytics

- Build queries from search results and events
- Apply group by and data aggregation on search results
- Perform CMDB and lookup table queries
- Perform nested query lookups

Section 2: FortiEDR Security Settings and Policies

- Configure communication control policy
- Configure security policies
- Configure playbooks
- Explain Fortinet Cloud Service (FCS)

Section 3: Rules and Subpatterns

- Identify various rule components
- Utilize rule subpatterns, aggregation, and group by
- Configure FortiSIEM analytics rules

Section 4: Incidents, Notifications, and Remediation

- Manage and tune incidents
- Configure notification policies
- Configure remediation options

Section 5: ML, UEBA, and ZTNA

- Configure machine learning configuration tasks
- Integrate UEBA data into rules and dashboards
- Describe ZTNA integration into FortiSIEM operations