FCP FortiAnalyzer Analyst

Cursusduur: 1 Dag **Cursuscode: ENFCPAN** **Trainingsmethode: Virtual Learning**

Beschrijving:

In this course, you will learn the fundamentals of using FortiAnalyzer for centralized logging. You will also learn how to identify current and potential threats through log analysis. Finally, you will examine the management of events, incidents, reports, and task automation with playbooks. These skills will provide you with a solid foundation for becoming a SOC analyst in an environment using Fortinet products.

Doelstelling:

- **After completing this course, you should be able to:**
- · Understand basic FortiAnalyzer concepts and features
- · Describe the purpose of collecting and storing logs
- · View and search for logs in Log View and FortiView
- · Understand SOC features
- · Manage events and event handlers
- · Configure and analyze incidents
- · Perform threat hunting tasks
- · Understand outbreak alerts
- · Describe how reports function within ADOMs
- · Customize and create charts and datasets
- · Customize and run reports
- · Configure external storage for reports
- · Attach reports to incidents
- · Troubleshoot reports
- · Understand playbook concepts
- · Create and monitor playbooks

Examens en certificering

Cursusinhoud:

Agenda:

1. Introduction and Initial Access
2. Logging
3. Incidents and Events
4. Reports
5. Playbooks

Nadere informatie:

Neem voor nadere informatie of boekingen contact op met onze Customer Service Desk 030 - 60 89 444

info@globalknowledge.nl

www.globalknowledge.com/nl-nl/

Iepenhoeve 5, 3438 MR Nieuwegein