FCP FortiAnalyzer Analyst

Duration: 1 Day **Course Code: ENFCPAN** **Delivery Method: Company Event**

Overview:

English - Please note this course is only available in English.
Nederlands - Let op: deze training is alleen in het Engels beschikbaar.
Franais - Veuillez noter que ce cours est uniquement disponible en anglais. 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.

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

Objectives:

- **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

Testing and Certification

Content:

Agenda:

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

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/