INFOSOFT IT SOLUTIONS

Training | Projects | Placements

Revathi Apartments, Ameerpet, 1st Floor, Opposite Annapurna Block, Infosoft It solutions,
Software Training & Development Institute, +91 - 9059683947 | +91 - 9182540872

FortiAnalyzer

Introduction to FortiAnalyzer

- Overview of FortiAnalyzer and its role in network security
- Key features and capabilities of FortiAnalyzer
- Comparison with other security information and event management (SIEM) solutions
- Use cases and benefits of deploying FortiAnalyzer in an organization

Installation and Setup

- System requirements and deployment options
- Installation procedures for FortiAnalyzer
- Initial configuration and setup wizard
- Licensing and registration

FortiAnalyzer Interface and Navigation

- Overview of the FortiAnalyzer user interface
- Navigation and layout of dashboards and menus
- Customizing views and preferences
- Access control and user management

Log Collection and Analysis

- Configuring log sources and collectors
- Supported log types and formats
- Real-time log monitoring and analysis
- Search and filtering techniques

Reporting and Alerting

- Pre-built report templates and customization options
- Scheduled reporting and email notifications
- Custom report creation and formatting
- Alerting mechanisms for security events

Log Retention and Archiving

- Log retention policies and best practices
- Archiving logs for long-term storage and compliance
- Compression and encryption options for archived data
- Retrieval and restoration of archived logs

Integration with Fortinet Products

- Integration with FortiGate for centralized logging and reporting
- Utilizing FortiAnalyzer with FortiManager for centralized management
- Integration with FortiSIEM for extended security analytics
- API and automation capabilities for integration with third-party systems

Advanced Analysis and Forensics

- Threat intelligence and incident response workflows
- Correlation and analysis of security events
- Forensic analysis tools and techniques
- Investigating security incidents using FortiAnalyzer

High Availability and Scalability

- High availability (HA) deployment options
- Load balancing and clustering for scalability
- Disaster recovery and failover configurations
- Performance tuning and optimization

Security Best Practices

- Security considerations for FortiAnalyzer deployments
- Role-based access control (RBAC) and user permissions
- Encryption and data protection measures
- Compliance with industry standards and regulations

Troubleshooting and Maintenance

- Diagnosing common issues with FortiAnalyzer
- Log management and storage optimization
- Upgrading and patching FortiAnalyzer software
- Backup and recovery procedures

Real-world Use Cases and Case Studies

- Examples of FortiAnalyzer deployments in different environments
- Case studies showcasing the benefits of FortiAnalyzer in security operations
- Practical exercises and scenarios for applying FortiAnalyzer features

FortiAnalyzer Certification Preparation

- Overview of Fortinet certification programs
- Exam preparation tips and resources
- Practice exams and quizzes
- Guidance on scheduling and taking certification exams

Conclusion and Next Steps

- Recap of key concepts covered in the course
- Opportunities for further learning and professional development
- Feedback and course evaluation
- Next steps for implementing FortiAnalyzer in your organization