Protecting Windows Servers and Embedded Systems

Zetlan Technologies

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Protecting Windows Servers and Embedded Systems

Course Modules

1.General

- Main functions of Kaspersky Security for Windows Server
- Kaspersky Security for Windows Server system requirements
- Protectn components of Kaspersky Security for Windows Servr
- Management & monitoring components of Kaspersky Security
- Licensing
- Main functions of Kaspersky Embedded System Security
- System requiremnts of Kaspersky Embedded Systems Security
- Protectn components of Kaspersky Embedded Systms Security
- Monitorg compnents of Kaspersky Embedded Systms Security
- Kaspersky Embedded Systems Security licensing
- Kaspersky Embedded Systems Security installation options

Protecting Windows Servers and Embedded Systems

2.Deployment

- Deployment order
- Quick Start Wizard
- List of installation packages
- Adjust the KSWS installation package settings (optional)
- Create a dedicated group for KSWS (optional)
  - o Prepare the Administration Server
- How to install Kaspersky Security for Windows Server
- Installation results
- Activating Kaspersky Security for Windows Server
  - o Install Kaspersky Security for Windows Server and Kaspersky
- Installing Kaspersky Security Console

3.Configuring group tasks

- Database Update task
- Application Module Update task
- On-demand scan tasks
  - o Configure Updates and on-demand Scanning

Protecting Windows Servers and Embedded Systems

4.File system protection

- Exploit Prevention
  - o Configurating Real-Time Protection
  - o Test Protection of Windows Subsystem for Linux
  - o Test Protection against exploits
- Anti-Cryptor
- How to configure Anti-Cryptor
- How to configure the blocking period for untrusted devices
  - o Configure Protection for Shared Folders
  - o Configuring the Anti-Cryptor Components

5.Network Threat Protection

- How Kaspersky Security for Windows Servr protcts from netwk
- How to configure Network Threat Protection
  - o Configure Network Threat Protection

Protecting Windows Servers and Embedded Systems

6.Protection for Remote Desktop Services

- Threat model for Remote Desktop Services sessions
- Traffic Security: Driver Interceptor
- Components of protection for Remote Desktop Services sessions
- Traffic Security: Redirector
- Traffic Security: External Proxy
  - o Configure Traffic Security in Driver Interceptor Mode
  - o Configure Traffic Security to scan mail traffic
  - o Configure Traffic Security to the External Proxy Mode

7.Server control components

- Applications Launch Control
  - o Enable Applications Launch Control in Test Mode
  - o Switch Application Startup Control into active Mode
  - o Create allow rules for installation packages and updates
- Device Control

8.System inspection

- File Integrity Monitor
- Log Inspection
  - o Configure the system Inspection Components

9.Protection for storages

- Storage protection capabilities
- Real-Time File Protection for storages
  - o Protect a NetApp Clustered Data ONTAP Storage
- Anti-Cryptor for NetApp
  - o Configure Anti-Cryptor for NetApp

10. Additional settings

- Protection for shared cluster resources
- Firewall Management
- SIEM integration
- Managing applications
- Collecting diagnostic information
- Monitoring the protection status (health check)

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474