HIRSCHMANN
A BELDEN BRAND

Network Security with Multi-Port EAGLE (SP3)

Today's industrial networks require maximum deployment flexibility as well as the highest security functionality. With multiple ports the EAGLE is ideally suited for creating Demilitarized Zones (DMZs). In addition the device is used to create multiple secure cells.

Target Group

Workshop for Technicians and Engineers who are involved with the security of an industrial network.

Prerequisites

An understanding of Ethernet and TCP/IP, for example "Industrial Ethernet (CT1)" and "Industrial Networking (CT2)" is required.
If available, the participant should bring a laptop with Ethernet connection and an operating system CD. Administrator rights are required.

Objective

In a professional environment the participants receive in-depth knowledge about the multi-port EAGLE and its security functionality. This includes installation, commissioning, and supervision. The training is part theory and part practice. The necessary knowledge about functions and deployment possibilities of the Tofino are taught in individual theory blocks. Each block is followed by practical exercises, designed to familiarize the participants with the devices through first-hand experience.

Languages

- SP3e English
- SP3d German

Duration

2 Days
9:00–16:30

Schedule / Location / Price

www.hicomcenter.com

Recommended for the Hirschmann™ Industrial Security Professional certification examination.

Seminar Content

Basic Settings

- HiDiscovery
- Software Management
- Configuration Management
- External Memory
- Port Configuration
- Time Synchronization

Swichting

- VLANs
- Prioritization (QoS)

Routing

- Port based Router Interfaces
- VLAN based Router Interfaces
- Static Routing

Device Security

- User Management
- Password Policy
- SNMP, Web, SSH access
- Restricted Management Access
- RADIUS

Network Security

- Filtering IP Packets
- 1:1 NAT
- Double NAT
- Masquerading NAT
- Destination NAT
- Denial of Service (DoS)
- Access Control Lists

Diagnostics

- Events
- Syslog
- Audit Trail
- Port statistics
- Topology Discovery
- Device Status
- Configuration Check