

# Network Security mit Multi-Port EAGLE (SP3)



## TRAINING FLYER

Heutige industrielle Netze benötigen ein Höchstmaß an Flexibilität bei der Implementierung als auch modernste Sicherheitsfunktionen. Mit bis zu 6 Ethernet-Ports ist der EAGLE ideal geeignet zum Aufbau von Demilitarized Zones (DMZs). Zusätzliche kann das Gerät zum Aufbau mehrerer Sicherheitszellen genutzt werden.

### Seminartyp und Zielgruppe

Produkttraining für Techniker und Ingenieure, die sich mit der Sicherheit von Industrienetzen befassen.

### Voraussetzungen

Grundkenntnisse im Bereich Ethernet und TCP/IP sind erforderlich, z. B. aus den Seminaren "Industrial Ethernet (CT1)" und "Industrial Networking (CT2)". Sofern vorhanden, sollte ein Laptop mit Ethernet-Schnittstelle, Betriebssystem-CD und Administrator-Recht mitgebracht werden.

### Zielsetzung

Die Teilnehmer erlernen den professionellen Umgang mit den Funktionen des Hirschmann Security Operating Systems (HiSecOS) der Produktfamilien EAGLE20/30 und EAGLE40, um die Komponenten selbstständig installieren, betreiben und warten zu können.

Das Training besteht aus Theorie- und Praxisteilen. In den Theorieblöcken wird das notwendige Fachwissen über die einzelnen Funktionen und Einsatzmöglichkeiten vermittelt. Anschließend machen sich die Teilnehmer in praktischen Übungen mit den Eigenschaften vertraut.

**Sprachversionen:** SP3d Deutsch, SP3e Englisch

**Dauer:** 3 Tage, je 9:00 - 16:30 Uhr

**Termine / Ort / Preis:**

[www.belden.com/resources/training](http://www.belden.com/resources/training)

Empfohlen zur Zertifizierung als Hirschmann Industrial Security Professional.

## Inhalt des Seminars

### Grundeinstellungen

- Software-Management
- Konfigurationsmanagement
- Externer Speicher
- Port-Konfiguration
- SHDSL-Ports
- Zeitsynchronisation

### Switching

- VLANs
- Priorisierung (QoS)

### Routing

- Port-basierte Router-Interface
- VLAN-basierte Router-Interface
- Statisches Routing
- OSPF
- Virtual Router Redundancy (VRRP)

### Gerätesicherheit

- Benutzerverwaltung
- Passwort Richtlinien
- SNMP-, Web-, SSH-Zugriff
- IP-Zugriffsbeschränkung
- RADIUS

### Netzsicherheit

- IP-Paketfilter
- 1:1 NAT
- Double NAT
- Masquerading NAT
- Destination NAT
- Denial of Service (DoS)
- Access Control Listen

### Virtuelle Private Netze (VPN)

- Authentisierung
- IKE
- IPsec
- Traffic Selektor

### Diagnose

- Ereignisse
- Syslog
- Audit Trail
- Persistente Logging
- Portstatistiken
- Topologie-Erkennung
- Gerätestatus
- Konfigurationscheck