



Sécurité Réseaux avec l'EAGLE Multi-ports (SP3)

Cible

Atelier pour les techniciens et les Ingénieurs impliqués dans la sécurisation d'un réseau industriel.

Pré-requis

Une connaissance d'Ethernet et de TCP/IP est requise, par exemple Ethernet industriel (CT1) et Réseaux industriels (CT2).

Si possible, le stagiaire doit apporter un ordinateur portable avec une connexion Ethernet et un CD du système d'exploitation. Les droits d'administrateur sont requis.

Objectif

Dans un environnement professionnel, les stagiaires reçoivent une connaissance approfondie sur l'EAGLE Multi-ports et ses fonctionnalités de sécurité. Ceci comprend l'installation, la mise en service et la supervision.

La formation est en partie théorique et pratique. Les connaissances nécessaires concernant les fonctions de sécurité et les possibilités de déploiement de l'EAGLE sont enseignées en blocs théoriques individuels. Chaque bloc est suivi d'exercices pratiques, pour familiariser les stagiaires avec les équipements par une prise en main directe

Les réseaux industriels d'aujourd'hui nécessitent une flexibilité de déploiement maximale ainsi que les plus hautes fonctionnalités en matière de sécurité. Avec ses ports multiples, l'EAGLE convient parfaitement pour segmenter différentes zones et créer des DMZ. De plus, l'appareil peut être utilisé pour isoler et sécuriser des cellules de production indépendantes.

Contenu de la formation

Réglages de base

- HiDiscovery
- Gestion des versions logicielles
- Gestion de la configuration
- Mémoire externe
- Configuration des ports
- Ports SHDSL
- Synchronisation horaire

Commutation

- VLAN
- Classement par priorité (QoS)

Routage

- Interfaces de routage par port
- Interfaces de routage par VLAN
- Routage statique
- OSPF
- Redondance de routeur virtuel (VRRP)

Sécurité de l'équipement

- Gestion des utilisateurs
- Stratégie de mot de passe
- Accès SNMP, Web et SSH
- Restrictions d'accès
- RADIUS

Réseaux privés virtuels (VPN)

- Authentification
- Paramètres IKE
- Paramètres IPsec
- Traffic Selectors



Sécurité réseau

- Filtrage des paquets IP
- NAT 1:1
- Double NAT
- Masquerading NAT
- Destination NAT
- Deni de service (DoS)
- Access Control Lists

Diagnostics

- Événements
- Syslog
- Audit Trail
- Journalisation persistante
- Statistiques ports
- Découverte de la topologie
- Etat des appareils
- Vérification de la configuration

Langues

- SP3e Anglais
- SP3d Allemand
- SP3f Français

Durée

3 jours
9:00 — 17:00

Calendrier / lieu / prix

www.hicomcenter.com



Recommandé pour l'examen de certification Hirschmann Industrial Security Professional.