

---

## Omnivise T3000 Cyber Security (K-T3CYSEC)

---

### Short Description

---

Cybersecurity and standards; maintenance of NIDS, whitelist application, monitoring configuration changes.

### Target Group

---

The target group of this workshop consists of customer IT personnel who are responsible/ interested in cyber security or for the administration and maintaining of security-features within Omnivise T3000 (e.g. security event monitoring, configuration-change management, application whitelisting etc.) Participants learn to understand why cyber security is important, the cyber security design of the network topology and the functionality and handling of security-event monitoring, configuration change monitoring and application whitelisting.

### Content

---

General cyber security Awareness  
Cyber security threats and attack vectors  
Discussion of the "threats" within the security cell by an insider  
Cyber security standard overview  
Explanation of the network topology/ security concept  
System Hardening/ Component security in Omnivise T3000  
Structural design and functionality of security-event monitoring \*\*  
Structural design and functionality of configuration-change monitoring  
Structural design and functionality of application whitelisting  
Live demonstration and exercises:  
• Creation and showing of events \*\*  
• Application Whitelisting Maintenance  
• Usage of configuration-change monitoring  
• Interpretation and hands-on in security-event monitoring \*\*  
• Network Intrusion Detection System Maintenance  
• Handling of cyber security incidents  
Note: The contents marked with \*\* based on release 8.2

### Prerequisites

---

Cyber Security basics, knowledge of information security and basic network technology

### Note

---

- Number of participants: max. 8
- Language: English
- Duration of course: 2 days
- Location of course: Training Center Karlsruhe

### Type

---

Classroom training

### Duration

---

2 days

### Language

---

en