Omnivise T3000 Cyber Security (K-T3CYSEC)

Target Group

Die Zielgruppe dieses Workshops sind IT-Mitarbeitern von Kunden, die in der Cybersicherheit oder für die Verwaltung und Pflege von Sicherheitsfunktionen innerhalb von Omnivise T3000 verantwortlich oder interessiert sind (z.B. Überwachung von Sicherheitsereignissen, Konfigurationsänderungsmanagement, Anwendungs-Whitelisting usw.). Die Teilnehmer lernen zu verstehen, warum Cybersicherheit wichtig ist, das Cybersicherheitsdesign der Netzwerktopologie und die Funktionalität und Handhabung von Sicherheitsereignisüberwachung, Konfigurationsänderungsüberwachung und Anwendungs-Whitelisting zu verstehen.

Content

Allgemeines Bewusstsein für Cybersicherheit
Cyber-Sicherheitsbedrohungen und Angriffsvektoren
Diskussion über die "Bedrohungen" innerhalb der Sicherheitszelle durch einen Insider
Überblick über die Cyber Sicherheitsstandards
Erläuterung der Netzwerktopologie/ des Sicherheitskonzepts
Systemhärtung / Komponentensicherheit in Omnivise T3000
Strukturelle Gestaltung und Funktionalität der Überwachung von Sicherheitsereignissen **
Strukturelle Gestaltung und Funktionalität der Überwachung von Konfigurationsänderungen
Strukturelle Gestaltung und Funktionalität der Anwendungs-Whitelisting
Demonstration und Übungen:
• Erstellung und Darstellung von Ereignissen **
• Pflege der Whitelist-Anwendung
• Verwendung der Überwachung von Konfigurationsänderungen
• Interpretation und praktische Übungen bei der Überwachung von Sicherheitsereignissen **
• Wartung des Netzwerk-Network Intrusion Detection Systems
• Behandlung von Cyber Sicherheitsvorfällen
Anmerkung: Die mit ** gekennzeichneten Inhalte basieren auf der Version 8.2

Prerequisites

keine; Empfohlen: Kenntnisse der Informationssicherheit und Netzwerktechnik

Note

- Teilnehmerzahl: max. 8
- Kurssprache: Deutsch; Sprachkenntnisse: Grundlagen Englisch erforderlich
- Kursdauer: 2 Tage
- Kursort: Trainingcenter Erlangen

Type

Face-to-face training

Duration

2 days

Language

de