OT300 OT Pentesting

Kurzbeschreibung:

Teilnehmende lernen die Grundlagen für Penetrationstests im OT-Umfeld kennen. Sie erfahren, wie Schwachstellen in Produktionsanlagen identifiziert werden und wie Penetrationstests helfen, das Sicherheitsniveau vernetzter OT-Umgebungen zu erhöhen. Der Kurs vermittelt praxisnahes Wissen, um OT als wichtigen Baustein der IT-Sicherheitsarchitektur abzusichern.

Zielgruppe:

- Blue Teams / Security-Teams / Security Practitioner
- IT- und Cybersecurity-Experten
- OT-Verantwortliche
- IT-Verantwortliche mit Bezug zu OT/Produktionsanlagen/Industriesteuerung
- IT- und OT-Fachleute, die ihre Fähigkeiten im Bereich OT-Pentesting erweitern möchten

Voraussetzungen:

Um den Kursinhalten und dem Lerntempo im Workshop **OT300 OT-Pentesting** gut folgen zu können, sind folgende Kenntnisse nötig:

- Grundlegende IT- und Netzwerk-Kenntnisse
- Grundkenntnisse im Bereich IT-Security

Hilfreich, aber nicht zwingend erforderlich sind darüber hinaus:

- Handlungssicherheit im Umgang mit Linux-Betriebssystemen
- Grundkenntnisse im Bereich Netzwerk-Protokolle
- Programmier-Grundkenntnisse Python
- Erfahrung im Umgang mit Virtualisierungsumgebungen (VMware, VirtualBox, o.vglb.)
- Erfahrung hinsichtlich der Durchführung von Security Assessments im IT-Umfeld

Sonstiges:

Dauer: 5 Tage

Preis: 3950 Euro plus Mwst.

Ziele:

Die Teilnehmer des Kurses **OT300 OT Pentesting** erlangen die theoretischen wie praktischen Grundlagen zur Planung, Umsetzung, Auswertung und Dokumentation von OT-Security Assessments/Penetrationstests, können diese in ausgewählten Testszenarien anwenden und auf eigene OT-Geräte oder ganze OT-Umgebungen (eigene Produktionsanlagen) übertragen.

Inhalte/Agenda:

- ♦ **Einführung OT, OT-Security, Pentesting**
  - ♦ ◊ Besonderheiten (OT vs. IT)
    ◊ Normen, Standards, Zertifizierungen
    ◊ Ziele, Ausprägungen/Abgrenzungen
    ◊ Wording
    ◊ Methodik

- ♦ **Praktische Umsetzung der vorgestellten Methodik**
  - ♦ ◊ Passive Informationsgewinnung/OSINT
    ◊ Aktive Informationsgewinnung
    ◊ Systemanalyse
    ◊ Angriffsszenarien

- ♦ **Physische Sicherheit**
  - ♦ ◊ Identifikation und Test von Schnittstellen
    ◊ Betriebsmodi

- ♦ **Firmware**
  - ♦ ◊ Grundlagen
    ◊ Firmwareanalyse

- ♦ **Reporting**
  - ♦ ◊ Schwachstellen bewerten und dokumentieren

- ♦ **Eigene Test-/Trainingsumgebung erstellen**

- ♦ **Capture The Flag (CTF) / Abschlussübung**
- ♦