SC175 NIS2 Lead Implementer

Kurzbeschreibung:

Teilnehmende lernen, die Anforderungen der NIS2-Richtlinie in bestehende Managementsysteme zu integrieren und daraus ein wirksames Cybersicherheitsprogramm abzuleiten. Behandelt werden Risikobewertung, technische und organisatorische Maßnahmen sowie Methoden zur Überwachung, kontinuierlichen Verbesserung und Auditierung, um die Umsetzung langfristig erfolgreich zu steuern und nachzuweisen.

Zielgruppe:

- Informationssicherheitsbeauftragte
- Risikomanager
- IT-Leitende
- Compliance-Verantwortliche
- Cybersecurity-Berater
- Fachkräfte in ENISA-Rollen: CISO, Cybersecurity Architect, Cyber Incident Responder

Voraussetzungen:

Sonstiges:

Dauer: 5 Tage

Preis: 2950 Euro plus Mwst.

Ziele:

- Den rechtlichen und regulatorischen Rahmen der NIS2-Richtlinie verstehen
- Verpflichtungen für wesentliche und wichtige Einrichtungen identifizieren
- Gap-Analysen und risikobasierte Priorisierungen durchführen
- Governance-, technische und organisatorische Maßnahmen umsetzen
- Verfahren zur Vorfallreaktion und Meldung etablieren
- NIS2-Anforderungen in bestehende Managementsysteme (z. B. ISO/IEC 27001) integrieren
- Rollenspezifische Kompetenzen gemäß ENISA Cybersecurity Skills Framework (ECSF) verstehen
- Die Cybersicherheitslage kontinuierlich überwachen und verbessern
- Als Rollenträger (CISO, Architect, Responder) zielgerichtet handeln

Inhalte/Agenda:

- ♦ **Grundlagen der NIS2 & regulatorischer Rahmen**
- ♦ ◊ Einführung in die NIS2-Richtlinie: Anwendungsbereich, Ziele, Neuerungen
  ◊ Rollen und Pflichten von Einrichtungen und Management
  ◊ Wesentliche vs. wichtige Einrichtungen: Kriterien und Anforderungen
  ◊ Überblick über nationale und europäische Aufsichtsstrukturen
  ◊ Durchführung einer NIS2-Gap-Analyse
  ◊ Einführung in ENISA ECSF und Rollenprofile
- ♦ ◊
- ♦ **Risikobasierte Planung & Governance-Strukturen**
- ♦ ◊ Methoden zur Risikobewertung und Priorisierung
  ◊ Business Impact Analyse & Schutzbedarfsfeststellung
  ◊ Governance- und Führungsverpflichtungen nach NIS2
  ◊ Aufbau eines Cybersecurity-Governance-Programms
  ◊ Vertiefung: CISO-Rolle – Aufgaben, Kompetenzen, Umsetzung
  ◊ Praxisübung: Entwicklung eines Governance Frameworks
- ♦ ◊
- ♦ **Sicherheitsmaßnahmen & technische Umsetzung**
- ♦ ◊ Technische und organisatorische Maßnahmen (Art. 21)
  ◊ Sichere Architekturen & Security by Design (Fokus: Architect)
  ◊ Sichere Softwareentwicklung und Cloud-Sicherheit
  ◊ Sicherheit in der Lieferkette und Drittparteien (Art. 21 Abs. 2d)
  ◊ Abgleich mit ISO/IEC 27001 Annex A
  ◊ Vertiefung: Architect-Rolle – Planung & Härtung
- ♦ ◊
- ♦ **Erkennung, Reaktion & Incident Management**
- ♦ ◊ Planung der Vorfallserkennung und Reaktion (Art. 23)
  ◊ Meldepflichten und Fristen (Art. 30)
  ◊ Aufbau eines SOC/CSIRT bzw. Meldeprozesses
  ◊ Vertiefung: Cyber Incident Responder – Aufgaben und Tools
  ◊ Fallstudie: Koordinierte Reaktion auf einen Cybervorfall
  ◊ Dokumentation, Forensik & Lessons Learned
- ♦ ◊
- ♦ **Audit, Awareness & kontinuierliche Verbesserung**
- ♦ ◊ Awareness- und Schulungsprogramme (Art. 20)
  ◊ Interne Kontrollmechanismen und Monitoring
  ◊ Berichtswesen gegenüber Management und Behörden
  ◊ Auditvorbereitung: Nachweisführung & Dokumentation
  ◊ Abschlussübung: Entwicklung einer rollenspezifischen NIS2-Roadmap
  ◊ Q&A, Feedback, Prüfungsvorbereitung
- ♦ ◊