Cybersecurity Incident - First Response.

Cybersecurity Incident - First Response.

Seminar | 3 Termine verfügbar | Teilnahmebescheinigung

Präsenz / Virtual Classroom | 7 Unterrichtseinheiten | Online durchführbar

Seminarnummer: 31185

Stand: 28.04.2024. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/31185

Reagieren Unternehmensverantwortliche richtig auf einen Einbruch in das IT-System oder beim Verdacht auf eine Manipulation des Systems? Im Vordergrund des Seminars steht die Informationsgewinnung und Einleitung von Sofortmaßnahmen, die eine Beweissicherung und -erhaltung ermöglichen. Da Manipulationen nicht immer sofort entdeckt werden, müssen auch mittelbare Schäden wie der Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen bei der Erarbeitung eines wirksamen Maßnahmenkataloges beachtet werden.

Nutzen

In diesem Seminar werden Strukturen erörtert, die eine Einbindung in das Notfall- und Krisenmanagement erleichtern. Die Teilnehmer des Seminars lernen unter anderem die Anwendung von Analyse-Software und -Tools, die Analyse von Schadsoftware, die Anatomie gezielter Angriffe sowie die ordnungsgemäße Dokumentation von Schäden, Angriffen und ergriffenen Maßnahmen. Teilnehmende erhalten Handlungsempfehlungen für die Einleitung von Sofortmaßnahmen bei Manipulationsverdacht

Zielgruppe

Technisch orientierte Mitarbeiter, wie

- Administratoren
- IT-Verantwortliche und Mitarbeiter, die in die Behandlung von Sicherheitsvorfällen einbezogen sind, wie Informationssicherheitsbeauftragte und Incident Manager
- IT- und Cybersecurity-Spezialisten

Voraussetzungen

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

Die Teilnahme ist nicht an formelle Voraussetzungen gebunden.

Inhalte des Seminars

- Grundlagen des Incident Managements
- Grundlagen der IT-Forensik
- Strategien zur Vorgehensweise, erste Schritte
- Einbindung in die Notfall- und Krisenorganisation
- Sicherung von Beweismitteln
- Live-Analyse und Post-Mortem-Abbild
- Ordnungsgemäße Dokumentation
- Forensische Duplikation von Daten
- Fundorte digitaler Spuren
- Analyse-Software und -Tools
- Anatomie gezielter Angriffe
- Ansätze zur Analyse von Schadsoftware

Wichtige Hinweise

- Das Seminar wird in Kooperation mit unserer langjährigen Tochtergesellschaft der isits AG in gewohnter TÜV-Rheinland-Qualität durchgeführt.

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/31185 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.