ConSecur Academy – IT-Security-Fachkräfte erfolgreich ausbilden

Von IT-Consultants und CDC-Managern aus der Praxis für die Praxis lernen – ConSecur Academy vermittelt das Wissen, als IT-Security-Analyst erfolgreich zu arbeiten. Kern unserer Fort- und Weiterbildungen ist seit jeher die Vorbereitung auf den sicheren, selbständigen Einsatz in der Praxis, Sicherheitsvorfälle zu analysieren und sicher zu dokumentieren.

„Selber laufen können", nennen wir das bei ConSecur.

ConSecur

[security and consulting]

TRAINING
zum Cyber Defense Analysten

Fachinformatiker und andere in IT-Berufen tätige Personen verstehen ihr Handwerk in der IT (Informationstechnik). Das Training „Cyber Defense Analyst“ aus der ConSecur Academy baut auf diesem Wissen auf.

Nach Abschluss dieser Intensivschulung in fünf Modulen werden Teilnehmer

- sensibilisiert sein für Informationssicherheit in ihren Unternehmen,
- Sicherheitsvorfälle erkennen, analysieren und auch gerichtsfest sauber dokumentieren sowie
- bei Anomalien selbständig erkennen, was zu tun ist, und er zu kontaktieren ist, um angemessene Maßnahmen in Abstimmung mit der hauseigenen IT einzuleiten

Inhaltlich behandelt die Schulung die Themen, die wir in der Ausbildung zum IT-Security-Analysten im Detail vermitteln.

AUSBILDUNG
zum 1st Level Security-Analysten

Sechsmonatige Ausbildung zum 1st Level Security-Analysten mit **praktischer und theoretischer Grundlagenvermittlung sowie einem „Training-on-the-Job“-Anteil im Cyber Defense Center (CDC).**

In den ersten drei Monaten erlernen die Teilnehmenden in fünf Modulen den fundierten theoretischen Hintergrund von IT- und Informationssicherheit, der auch die vorhandene IT-Infrastruktur sowie Besonderheiten wie regulatorische Vorgaben beinhaltet.

Im ebenfalls dreimonatigen Training-on-the-Job“-Anteil erwerben die künftigen IT-Security-Analysten die praktische Erfahrung, im Cyber Defense Center als 1st Level Security-Analyst sicher zu agieren.

Von der ConSecur Academy ausgebildete IT-Security-Analysten werden die Kompetenzen besitzen, im Cyber Defense Center potentielle Sicherheitsvorfälle nach verbindlichen Regeln zu identifizieren, zu analysieren und zu dokumentieren.

Muster erkennen und dahinterkommen – ausgebildete IT-Security-Analysten beschäftigen sich im CDC mit dem Denken der anderen.

INDIVIDUALISIERTE AUSBILDUNGEN

Unter Berücksichtigung unternehmensspezifischer Vorgaben und Gepflogenheiten

Die Module

MODUL 1 – Grundlagen Informationssicherheit

Ordnen wir Definitionen, Begrifflichkeiten und Standards ein. Im ersten Modul beschäftigen wir uns mit Grundlagen der Informationssicherheit, sodass wir darüber ein gemeinsames Verständnis besitzen und dieselbe Sprache sprechen. Was ist die Cyber Kill Chain noch mal und wie läuft ein Hack eigentlich ab? **Wir werden es erfahren!**

MODUL 2 – Defense in Depth

Es geht um Sicherheitsbewusstsein und um Verteidigungskonzepte im Detail. Wie funktionieren Virenscanner und Intrusion Detection Systeme? Welches Konzept steckt dahinter und gegen welche Angriffe wirken sie und gegen welche nicht? Im zweiten Modul reden wir auch über den Faktor Mensch innerhalb der Informationssicherheit.

MODUL 3 – Kommunikationsprotokolle

Sprechen wir über Netzwerke und Kommunikationswege. Welche Netzwerkprotokolle gibt es und welche Informationen verbergen sich darin? Wir beschäftigen uns mit dem Aufbau gängiger Netzwerkprotokolle und können im Anschluss an Modul 3 auch sicher folgende Frage beantworten: Was haben Kommunikationsprotokolle mit Informationssicherheit zu tun und warum sind diese anfällig für Angriffe?

MODUL 4 – Malware

Malware hat viele Gesichter. Wir schauen uns Schadsoftware verschiedener Ausprägungen an, werden ihre Funktionsweise und ihre Auswirkungen verstehen und zeigen, wie das raffinierte EMOTET ganze Infektionsketten bildet und dabei Endgeräte und Unternehmensnetzwerke auskundschaftet. Die Fähigkeit, Malware-Infektionen ohne AV- oder Endpoint-Detection-Lösungen zu erkennen, erwerben wir auch.

MODUL 5 – Grundlagen des Incident Handlings

Was machen wir, wenn es passiert ist? Wir beschäftigen uns mit Incidents, die uns als Anomalie begegnet sind, und sich als Sicherheitsvorfall entpuppt haben. Wie gehen wir damit um? Welche Maßnahmen ergreifen wir? Wir werden mit zielgerichteten Lösungen vertraut sein.

ConSecur

[security and consulting]

ConSecur GmbH
Nödiker Straße 118
49716 Meppen

TEL.: +49 5931 9224-0
info@ConSecur.de
www.ConSecur.de