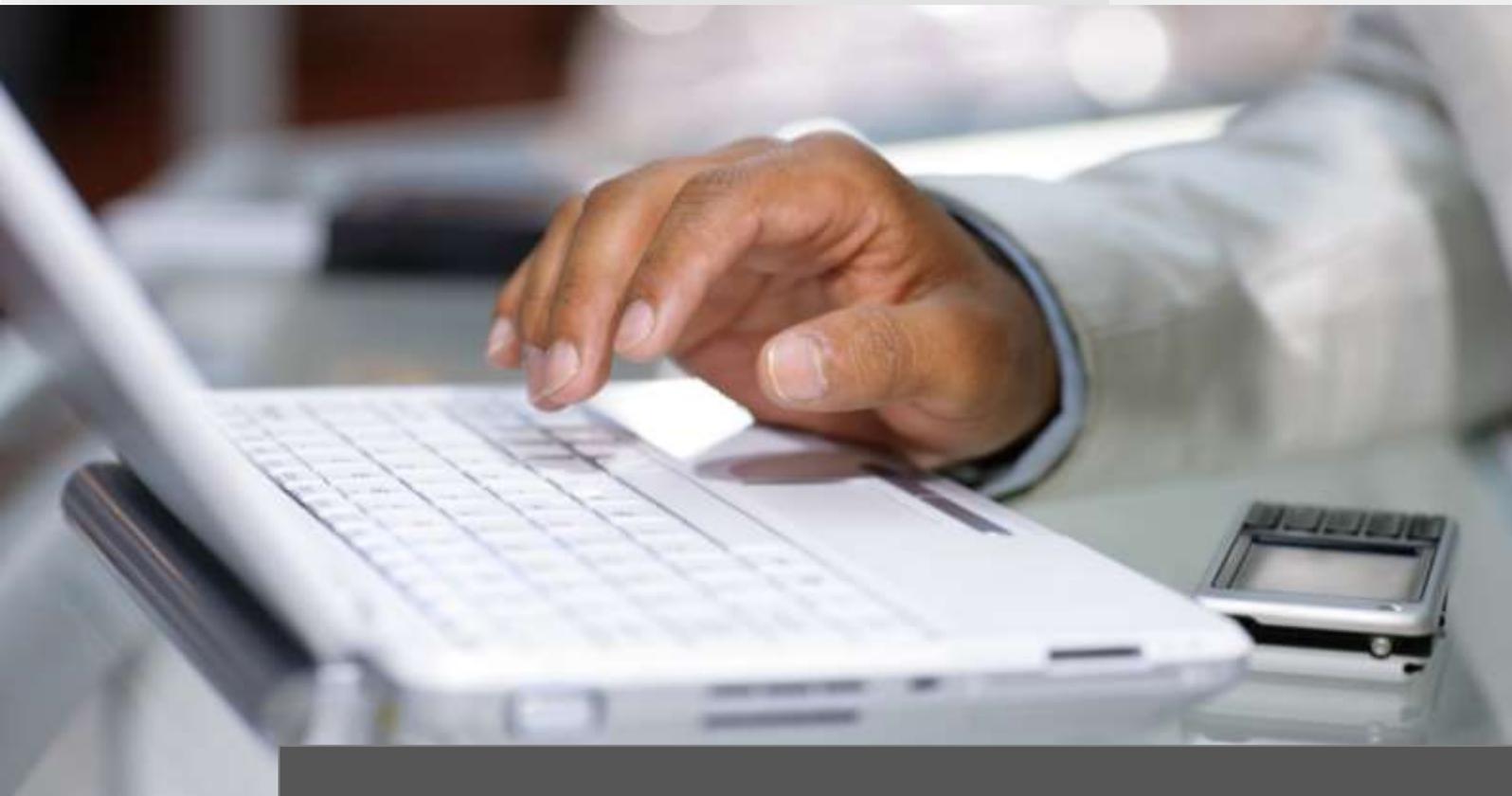


Certified PC Forensic Professional

Online-Training | Examen CFP



Ausbildungsinhalte

Technische Trainings

Certified PC Forensic Professional

Ausbildungspfad | Certified Forensic Expert



Nach dieser Ausbildungsreihe haben Sie die Möglichkeit durch „Aufklärung eines Real World Szenarios“ eine sehr praxisorientierte Zertifizierungsprüfung zum *Certified PC Forensic Professional* abzulegen.

Online-Training	Dauer	Examen
Certified PC Forensic Professional	20 UE	CSH

Sie erlernen unter anderem gelöschte Dateien wiederherzustellen, einen Aktivitätsindex zu erstellen, E-Mails, Binärcodes, die Registry und Datenbanken zu analysieren, versteckte Bereiche aufzudecken, Password Recovery, Angriffe gegen Bitlocker und vieles mehr.

Auch rechtliche Aspekte und die Durchführung von forensischen Sicherungen inklusive verschiedenen Sonderfällen (z.B. RAID oder SSD-Speichermedien) sind Bestandteil der Ausbildungsreihe.

Unterrichtseinheit	UE 01	CPFP
Einführung und Hintergründe <ul style="list-style-type: none"> ✓ Geschichte der Computer Forensic ✓ Erfolge der Computer Forensic ✓ Ein Thema für jeden? <ul style="list-style-type: none"> ▪ Privatpersonen ▪ Unternehmen ▪ Öffentlicher Dienstag ✓ Unterstützende Gesetze <ul style="list-style-type: none"> ▪ IT-Sicherheitsgesetz ▪ Bundesdatenschutzgesetz ▪ Strafgesetzbuch ✓ Forensic im Internet <ul style="list-style-type: none"> ▪ Forensic Tools in diesem Training ▪ OSForensics ▪ Volatility ▪ Sonderfall: Mobile Device Forensic ✓ Formen der Computer Forensic <ul style="list-style-type: none"> ▪ Live Response ▪ Post Mortem 		

Unterrichtseinheit	UE 02	CPFP
Cybercrime – Zahlen , Fakten und Fallbeispiele ✓ Cyberkriminalität in Deutschland (2010 – 2015) ✓ Schäden durch Cyberkriminalität ✓ Forensische Methoden im Unternehmen ✓ Grundsätzliches ✓ Erstmaßnahmen treffen ✓ Szenario <ul style="list-style-type: none"> ▪ Hackerangriff I - IV ▪ Hackerangriff Website ▪ Hackerangriff Mitarbeiter (HeimPC) ▪ Hackerangriff Ransomware ▪ CEO Fraud ▪ CEO Fraud II ▪ Erpressung 		

Unterrichtseinheit	UE 03	CPFP
Forensische Verfahren im Überblick – Live Response ✓ Einführung ✓ Vorbereitung ✓ Vorbereitung II ✓ Analyse des betroffenen Systems ✓ Vorteile des Speicherdumps ✓ Live Response mit OS Forensics ✓ Beispiel <ul style="list-style-type: none"> ▪ Prozess und Speicheranalyse ▪ Gelöschte Dateien lokalisieren ✓ Schnellüberblick		

Unterrichtseinheit	UE 04	CPFP
Forensische Verfahren im Überblick – Post Mortem Forensik ✓ Einführung ✓ Vorbereitung ✓ Vorbereitung II ✓ Vorbereiten für Post Mortem Forensiken ✓ Erstellung eine forensischen Kopie ✓ Integration von forensischen Kopien ✓ Erste Schritte am forensischen Image ✓ Schnellüberblick		

Unterrichtseinheit	UE 05	CPFP
Einführung: OSForensics ✓ Hintergrund ✓ Drei Phasen Anwedung ✓ Weitere Features: <ul style="list-style-type: none"> ▪ Hash-Set Unterstützung ▪ Rainbow Tables ✓ Trainings und Zertifizierungen ✓ Zusammenfassung		

Unterrichtseinheit	UE 06	CPFP
Forensische Datenträgersicherung <ul style="list-style-type: none"> ✓ Grundlagen ✓ Methode <ul style="list-style-type: none"> ▪ Physikalische Kopie ▪ Physikalische Kopie – Writeblocker ▪ Logische Kopie – Bordmittel ▪ Logische Kopie – Bordmittel II ✓ Verifikation einer Forensischen Kopie ✓ Abhängigkeit vom Betriebssystem ✓ DEFT Linux <ul style="list-style-type: none"> ▪ Überblick ▪ Forensische Kopie mit Guymager ✓ Forensische Kopie mit OSForensics ✓ Image-ing Special: .E01 nach VMDK ✓ Sonderfall: Mobile Endgeräte ✓ Beispiel: Elcomsoft Phone Password Breaker 		

Unterrichtseinheit	UE 07	CPFP
Forensic Discovery <ul style="list-style-type: none"> ✓ Angriffe gegen Bitlocker Medien <ul style="list-style-type: none"> ▪ Zwingende Voraussetzung ▪ Problematik ▪ Angriffsszenarien ▪ Notwendige Tools ✓ Live Demo: Elcom Forensic Disk Decrypter ✓ Verschieden Ziele zur Auswahl ✓ Einstieg in die Forensic Discovery / OS Forensic <ul style="list-style-type: none"> ▪ Suche nach Daten ▪ Erzeugen von Verzeichnissignaturen 		

Unterrichtseinheit	UE 08	CPFP
Forensic Discovery <ul style="list-style-type: none"> ✓ Forensische Analyse <ul style="list-style-type: none"> ▪ Real World ✓ Einleitend <ul style="list-style-type: none"> ▪ Prüfsummenverifikation ✓ Alternativ <ul style="list-style-type: none"> ▪ Prüfsummenverifikation ✓ Case für Data Leakage erstellen ✓ Zielvorgaben Data Leakage Case 		

Unterrichtseinheit	UE 09	CPFP
Forensic Discovery <ul style="list-style-type: none"> ✓ Realistische Aufwände und Zahlen ✓ Special: Mobile Device Forensic ✓ Live Demo 		

Unterrichtseinheit	UE 10	CPFP
Forensic Identify – RAID/NAS Recovery <ul style="list-style-type: none"> ✓ Problemsituation: RAID/NAS Recovery ✓ Praxisbeispiel <ul style="list-style-type: none"> ▪ LINUX RAID ▪ LINUX RAID bei OS Forensics ✓ Alternative Lösung <ul style="list-style-type: none"> ▪ R-Studio von RTT ✓ Problemlösung <ul style="list-style-type: none"> ▪ FTK Imager & R-Studio = RAID/NAS Recovery ✓ Fertiges Image bearbeiten 		

Unterrichtseinheit	UE 11	CPFP
<p>Forensic Identify – Typische Kundenanfrage</p> <ul style="list-style-type: none"> ✓ Vorbereitung/Vorspiel ✓ OS Forensic Vorbereitung ✓ Suche nach Verborgenen ✓ Rekonstruktion nach Graden ✓ Ungewöhnliche Dateien finden ✓ Gezielte Zeiträume 		

Unterrichtseinheit	UE 12	CPFP
<p>Forensic Identify – Memory Forensic</p> <ul style="list-style-type: none"> ✓ Schnelle Einblicknahme ✓ Problematik ✓ Volatility Framework <ul style="list-style-type: none"> ▪ Schnellüberblick ▪ Hiberfil.SYS Wandlung ▪ Im Einsatz ✓ Logische Angriffe für Memory Acces ✓ Inception – Memory Attacks 		

Unterrichtseinheit	UE 13	CPFP
<p>OS Forensics – Erstellen von Berichten</p> <ul style="list-style-type: none"> ✓ Berichterstellung ✓ Memory Forensic ✓ OS Forensic <ul style="list-style-type: none"> ▪ Bericht erstellen ▪ Integration von Beweisbildern ▪ Integration in Bericht ▪ Überblick Anpassung OS Forensics Reports 		

Unterrichtseinheit	UE 14	CPFP
<p>OS Forensics – Password Breaking</p> <ul style="list-style-type: none"> ✓ Knacken von Passwörtern mit OS Forensics ✓ Integrierte Möglichkeiten <ul style="list-style-type: none"> ▪ Password ▪ Keys ✓ Windows Kennwörter <ul style="list-style-type: none"> ▪ Lokal ▪ Domain ✓ Rainbow Tables mit OS Forensics erzeugen ✓ Rainbow Tables <ul style="list-style-type: none"> ▪ Downloaden ▪ Einsetzen ✓ Dateien im OS Forensics knacken ✓ Kommerzielle Recovery Tools ✓ NIST National Software Reference Library (NSRL) ✓ NSRL im Überblick ✓ Integration von RDS nach OS Forensics ✓ Einsatz von NSRL (RDS 2.55 Modern Unique) 		

Unterrichtseinheit	UE 15	CPFP
Forensische Malware Analyse <ul style="list-style-type: none"> ✓ Analyse von Malware ✓ Kompaktes Malware 1&1 ✓ Forensischer Ansatz <ul style="list-style-type: none"> ▪ Malware Analyse ✓ Online-AV-Scan (oder Filezugriff & Vtotal) ✓ Offline-AV-Scan (Virtualisierung des Images) ✓ Offline-AV-Scan (AV Scan innerhalb VM) ✓ Memory Forensik (Anti Malware Methoden) ✓ Einsatzgebiete 		

Unterrichtseinheit	UE 16	CPFP
Spearphishing Angriff im Detail <ul style="list-style-type: none"> ✓ Überblick ✓ Einführung Testumgebung ✓ Forensische Analyse 		

Unterrichtseinheit	UE 17	CPFP
Darknet Aktivität am Arbeitsplatz <ul style="list-style-type: none"> ✓ Überblick ✓ Einführung Testumgebung ✓ Schritte im Detail ✓ TOR Konfigurationsdateien ✓ Forensische Analyse <ul style="list-style-type: none"> ▪ Memory Forensik ▪ Post Mortem Forensik ✓ Forensik Remount <ul style="list-style-type: none"> ▪ VM-gestützter Zugriff 		

Unterrichtseinheit	UE 18	CPFP
Forensische Berichterstattung: Anforderung & Special: AntiForensik <ul style="list-style-type: none"> ✓ Forensische Analyse erschweren ✓ Verschleierung von Informationen ✓ Verschlüsselung von Informationen ✓ Manipulation von Zeitinformationen (Win) ✓ Komplette Zerstörung von Informationen ✓ Szenario <ul style="list-style-type: none"> ▪ Schlagwortsuche ▪ Malwareanalyse ✓ Ausgang einer Forensik ✓ Rechtsstreit ✓ Beweis in der Forensik ✓ Mitarbeiter als Täter – zu beachten ✓ Ermittlungsmethoden gegen Mitarbeiter ✓ 1&1: Was tun bei illegalen Datenfund? 		

Unterrichtseinheit	UE 19	CPFP
Forensische Berichterstattung: Ausführung und Umsetzung <ul style="list-style-type: none"> ✓ Dokumentation im Überblick ✓ Deckblatt ✓ Inhaltsverzeichnis ✓ Executive Summary ✓ Forensische Sicherung <ul style="list-style-type: none"> ▪ Wann/wo durchgeführt? ▪ Wer war anwesend? ▪ Welche Tools wurden eingesetzt? ▪ Welche Beweisstücke wurden eingesetzt? ▪ Fotos der Beweisstücke ✓ Definition der Untersuchungsmethoden 		

	Unterrichtseinheit	UE 20	CPFP
	<p>Forensische Berichterstattung: Ausführung und Umsetzung</p> <ul style="list-style-type: none">✓ Dokumentation im Überblick✓ Ereignis: Funde nach Schlagwortliste✓ Special: Beispiel Memory Forensik✓ Abschlussnotiz✓ Einblick Netzwerk-Forensik		



Weitere wichtige Informationen

Ihr Trainer: Herr Thomas Wittmann

Der Trainer dieser exklusiven Online-Ausbildungsreihe ist Herr Thomas Wittmann. Er ist ca. 20 Jahren im Bereich IT-Security aktiv und als *Senior Security Specialist* für innoSec | Schweiz tätig. Er ist einer der erfahrensten Sicherheitsexperten Deutschlands!

Neben einer umfangreichen Praxiserfahrung trägt er unter anderem die Titel *Professional Security Analyst Accredited Certification (OPSA)*, *Professional Security Tester Accredited Certification (OPST)* und *Offensive Security Certified Professional (OSCP)*. Zudem ist er als Oracle Datenbank-Spezialist, System-administrator und Datenschutzbeauftragter aktiv. Hierüber hinaus verfügt er über sehr viel Erfahrung als national und international tätiger Penetrationstester und dies auch in hochkritischen Bereichen wie beispielsweise regierungsnahen Umgebungen.

Als „Ex-Hacker“ gab er 2012 dem Handelsblatt ein Interview, in dem er die Bedrohungslage für Start-ups aufzeigte. 2016 nahm er im WDR Stellung zum Hackerangriff auf die Telekom.

Optimale Prüfungsvorbereitung

Etwa ein zwei Tage vor der Prüfung zum *Certified PC Forensic Professional* erhalten Sie alle notwendigen Prüfungsunterlagen und eine detaillierte Anleitung, wie Sie die Prüfung ablegen können und was das Ziel Ihres Angriffs ist.

Sie haben Fragen oder Anregungen?

Falls Sie Fragen, Wünsche oder Anregungen zu dieser oder zu anderen Ausbildungen haben, stehen wir Ihnen montags bis donnerstags in der Zeit von 08:00 – 17:00 Uhr und freitags von 08:00 – 15:00 Uhr sehr gerne zur Verfügung.

Sie erreichen uns unter:

Telefon: 09526 95 000 60
E-Mail: info@ITKservice.NET

Ihre Ansprechpartner für das ITKwebcollege.Security Hacker

Christoph Holzheid
Anne Hirschlein
Thomas Wölfel



Copyrights und Vertragsbedingungen

Das Copyright © aller Trainings, inkl. aller Aufzeichnungen und Unterlagen obliegt der ITKservice GmbH & Co. KG. Die Nutzung aller ITKwebcollege-Leistungen ist nur für den Vertragspartner und nur für den internen Gebrauch gestattet. Eine Weitergabe der Leistungen an Dritte ist nicht zulässig.

Kontaktdaten | Impressum

ITKservice GmbH & Co. KG

Fuchsstädter Weg 2
97491 Aidhausen

Telefon: 09526 95 000 60

Telefax: 09526 95 000 63

www: ITKservice.NET

E-Mail: info@ITKservice.NET

Sitz der Gesellschaft: Aidhausen | Amtsgericht Bamberg, HRA 11009, Ust-Id: DE 262 344 410 | Vertreten durch: Thomas Wölfel (GF).

Bildnachweise: Alle in diesem Dokument dargestellten Bilder wurden von der ITKservice GmbH & Co. KG bei ccvision.de lizenziert.

Redaktion: ITKservice GmbH & Co. KG | Copyright © 2017 ITKservice GmbH & Co. KG.