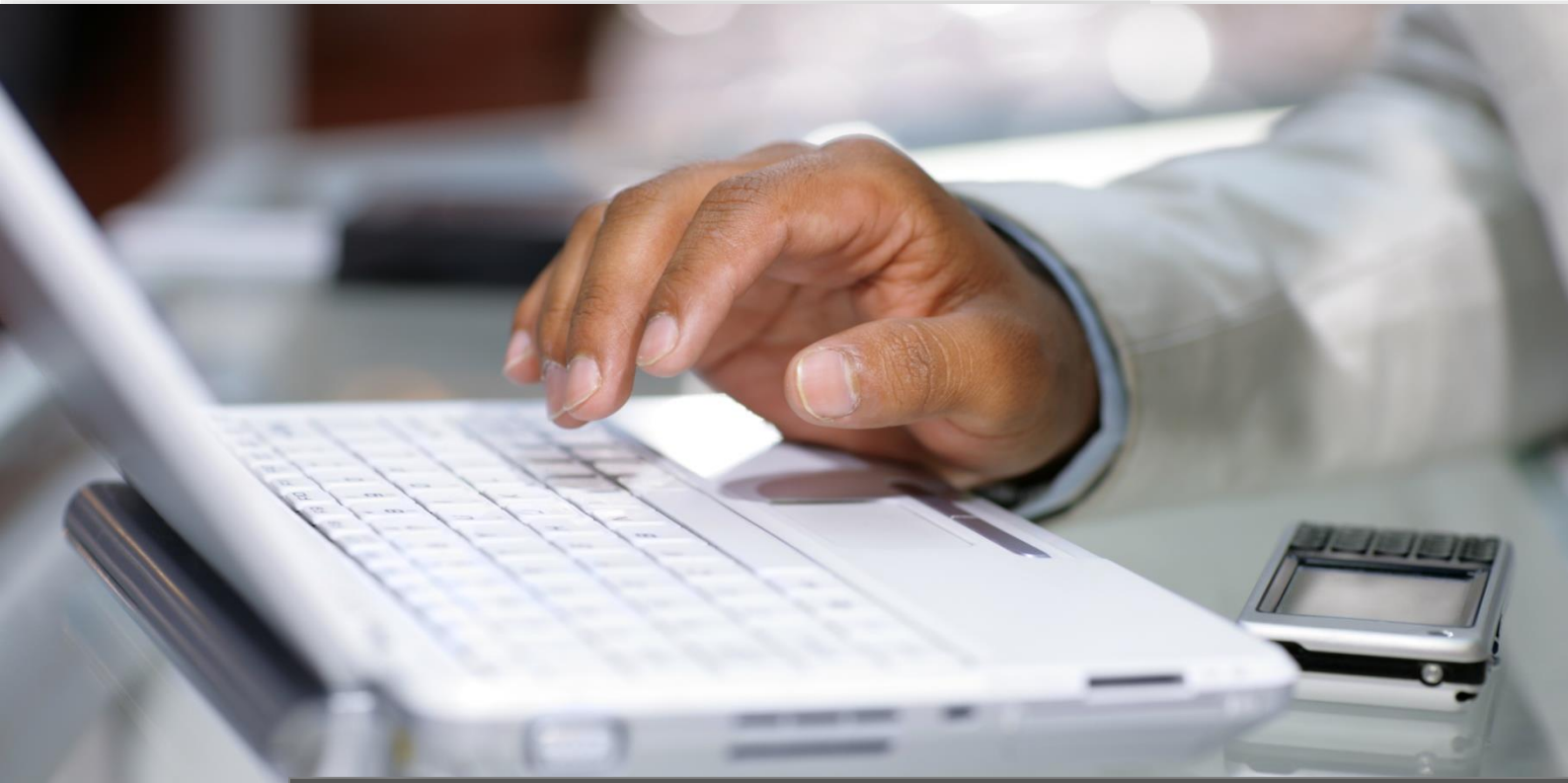
Certified Network Forensic Professional

Online-Training | Examen CNFP



Ausbildungsinhalte

ITKservice

Certified Network Forensic Professional

Ausbildungspfad | Certified Forensic Expert

CPFP → CNFP → CFE Certified Forensic Expert

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

	Online-Training	Dauer	Examen
	Certified Network Forensic Professional	20 UE	CNFP

Aufbauend auf dem Wissen der PC-Forensik lernen Sie Bedrohungsszenarien kennen, lernen Datenströme im Netzwerk zu analysieren und Netzwerksensoren einzurichten. Sie führen verschiedene Real World Szenarios durch und erhalten die Kenntnisse forensische Berichte zu erstellen.

	Unterrichtseinheit	UE 01	CNFP

Einführung und Hintergründe
- ✓ Definition
  - Teilgebiet
  - Digital Forensics
  - Network Traffic Analyse
  - Intrusion Detection
- ✓ Entstehungsgeschichte
  - Netzwerk Forensik
- ✓ OSI Schichtenmodell – Kurzüberblick
- ✓ Einfache Beispiele vs Unternehmensstrom
- ✓ Hohe Datenvolumen und Analyse
- ✓ Security Onion
  - Kurzüberblick
  - Tools im Überblick
  - Forensic & NSM Linux

	Unterrichtseinheit	UE 02	CNFP

Cyberkriminalität, Network Forensik, Szenarien & Fallbeispiele
- ✓ Cybercrime & Bedrohung im Unternehmen
- ✓ Abwehr/Erkennung Industriespionage
  - Früherkennung
  - Späterkennung
- ✓ Datendiebstahl durch Mitarbeiter
- ✓ Ransomware
- ✓ DDoS Angriffe (Erpressung)
- ✓ CEO Fraud Angriffe
- ✓ Die Drei wichtigsten Tools
  - Squil
  - Squert
  - ELSA

	Unterrichtseinheit	UE 03	CNFP

Analyse von Datenströmen im Unternehmensnetzwerken
- ✓ Grundvoraussetzungen
- ✓ Einfaches Netzwerk
  - Musterlösung
  - Gängige Praxis
- ✓ Komponenten der Security Onion
- ✓ Problematik
- ✓ Schutzbedarf durch NSM
- ✓ Arbeitsplätze
  - DMZ
  - Wireless LANs
  - Server/Infrastruktur
- ✓ NSM Planphase 1
- ✓ Technische Mittel zur Integration von Sensoren
- ✓ Port Mirroring
- ✓ Network Tap
- ✓ NSM Testumgebung

Unterrichtseinheit	UE 04	CNFP

Grundlagen Netzwerk Datenstromanalyse
- ✓ Basic Tools
  - TCPDump
  - Wireshark
- ✓ Advanced Tools
  - Netsniff-NG

- ✓ Quellen für PCAPS im Internet
- ✓ Wireshark PCAP Samples
- ✓ Einstieg
- ✓ Einfach Mitschnitt
- ✓ Grundlagen
  - Aufzeichnungen mit TCPDump
  - Einspeisen von Aufzeichnungen
  - Filterung von Mitschnitten

Unterrichtseinheit	UE 05	CNFP

Grundlagen Netzwerk Datenstromanalyse II
- ✓ Basic Tools
  - Wireshark
  - CAP Analysis
  - IP Geolocation Services

- ✓ Statistische Daten
  - Wireshark
  - CAP Analysis
  - Fortgeschrittene Protokollanalysen
  - IP Geolocation Services
- ✓ Einsatzbeispiele
  - Forensische Analyse Hackerangriff
  - Security Onion

Unterrichtseinheit	UE 06	CNFP

Grundlagen Netzwerk Datenstromanalyse III
- ✓ Basic Tools
  - Wireshark
  - Security Onion

- ✓ Fortgeschrittene Analysen mit Wireshark
- ✓ Anleitung für Mitschnitte
- ✓ Prüfsummen für PCAPs erstellen
- ✓ Einspeisung Security Onion

Unterrichtseinheit	UE 07	CNFP

Aufbau eines Analysesystems Security Onion (1)
- ✓ Security Onion
  - Download und Installation
  - Spezielle Vorbereitung: Ethernet Interfaces
  - Erste Schritte
    - Updates
    - Grundinitialisierung
    - Grundfunktionsüberprüfung

Unterrichtseinheit	UE 08	CNFP

Aufbau eines Analysesystems Security Onion (2)
- ✓ Security Onion
  - Download und Installation
  - Stand Alone Installation
  - Server/Sensor Installation

Unterrichtseinheit	UE 09	CNFP

Netzwerk Forensic Tools - Einführung
- ✓ Primäre Tools Security Onion
  - SNORT (IDS)
  - Xplico/Netminer (Network Forensic)
  - Sguil/Squert (Network Security Analysis)
  - ELSA/Bro (Log Management)
  - Argus/RA (Network Dataflow Analysis)

Unterrichtseinheit	UE 10	CNFP

Netzwerk Forensic Tools - Einführung

- ✓ Snort
  - Historie
  - Community Rules
  - Registered User Rules
  - Subscriber Release Rules
  - Emerging Thread (ET) Rules
  - Emerging Thread (ET) Daily Updates
  - Beispiel: Malware Zeus
  - Security Onion und Snort Rules
  - Snort Rules und Alerts
- ✓ Xplico
  - Übersicht
  - Features

Unterrichtseinheit	UE 11	CNFP

Netzwerk Forensic Tools - Advanced

- ✓ Squil
- ✓ Squert
- ✓ ELSA

Unterrichtseinheit	UE 12	CNFP

Netzwerk Forensic Tools – Advanced

- ✓ Analyse Szenario
  - Squil
  - Squert
  - ELSA

Unterrichtseinheit	UE 13	CNFP

Real World: Spearphishing / CEO Fraud

- ✓ Übersicht
  - Spearphishing
  - CEO Fraud
- ✓ Analyseansatz: E-Mail
- ✓ Bespielheader (Realer Angriff)
- ✓ Header Extraktion
  - Received Ziele
  - ISP Ermittlung
- ✓ Technische Ansätze zur Alamierung
- ✓ Bro Sensor
  - ELSA (Nachanalyse)
  - Snort/IDS (Frühwarnsystem – Echtzeit)

Unterrichtseinheit	UE 14	CNFP

Real World: Backdoors und Exploits erkennen

- ✓ Übersicht
  - Spearphishing
- ✓ Download und Installation: Security Onion
- ✓ Primäre Tools in Security Onion
  - SNORT (IDS)
  - Xplico / Netminer (Network Forensic)
  - Sguil / Squert (Network Security Analysis)
  - ELSA / Bro (Log Management)
  - Argus / RA (Network Dataflow Analysis)
- ✓ Übersicht
  - Exploit
- ✓ Kategorien von Exploit
  - Local Exploits
  - Local Privilege Escalation Exploits
  - Remote von Exploits
  - SONDERFÄLLE: Elternal Blue Exploits
  - Pass the Hash Angriffe
- ✓ Sonderfall: Domain Angriffe
  - AS Requests per Kerberus

Unterrichtseinheit	UE 15	CNFP

Real World: Analyse von Angriffstunneln
- ✓ Network Forensic Exploits, BD's und Tunnel
- ✓ Primäre Tools in Security Onion
  - SNORT (IDS)
  - Xplico / Netminer (Network Forensic)
  - Sguil / Squert (Network Security Analysis)
  - ELSA / Bro (Log Management)
  - Argus / RA (Network Dataflow Analysis)
- ✓ Übersicht
  - Pass-the-Hash Angriff
  - Kerberos Analysen in Security Onion
- ✓ Tunnel Verfahren
  - IODINE (DNS Tunnel)
  - HANS (ICMP Tunnel)

Unterrichtseinheit	UE 16	CNFP

Network Forensic Report (Generell)
- ✓ Basis Voraussetzung
- ✓ Security Onion
- ✓ Primäre Tools in Security Onion
  - SNORT (IDS)
  - Xplico / Netminer (Network Forensic)
  - Sguil / Squert (Network Security Analysis)
  - ELSA / Bro (Log Management)
  - Argus / RA (Network Dataflow Analysis)
- ✓ Empfohlene Tools
- ✓ CAP Analysis
- ✓ Graylog
- ✓ Beispielbericht
- ✓ Weiterer Beispiele für Berichtsinhalte

Unterrichtseinheit	UE 17	CNFP

Network Forensic Report (Fortsetzung)
- ✓ Basis Voraussetzung
- ✓ Security Onion
- ✓ Primäre Tools in Security Onion
  - SNORT (IDS)
  - Xplico / Netminer (Network Forensic)
  - Sguil / Squert (Network Security Analysis)
  - ELSA / Bro (Log Management)
  - Argus / RA (Network Dataflow Analysis)
- ✓ Empfohlene Tools
- ✓ CAP Analysis
- ✓ Graylog
- ✓ Special: Einfacher Zugriff auf Security Onion
- ✓ Offline Anti Virus Scan
- ✓ Beispielbericht
- ✓ Weiterer Beispiele für Berichtsinhalte

Unterrichtseinheit	UE 18	CNFP

Special: NSM vs. Emotet v4 & Feodo
- ✓ Emotet
  - Bekannte Angriffsmethoden
  - E-Mail Abwehrverfahren
  - Windows Defender Spread
  - Modifikation von Emotet
  - NSM Simulation von Emotet
  - Abwehrmaßnahmen

	Unterrichtseinheit	UE 19	CNFP
	Rechtliche Aspekte zu Netzwerk Forensik ✓ Fallszenarien ▪ Hackerangriff (I – II) ▪ CEO Fraud ▪ Malware Infektion (I – III) ▪ Mitarbeiter Datendiebstahl (I – II) ✓ Ausgang einer Forensik ✓ Rechtsstreit ✓ Beweise in der Forensik ✓ Mitarbeiter als Täter – zu beachten ✓ Ermittlungsmethoden gegen Mitarbeiter ✓ 1&1: Was tun bei illegalen Fund?		

	Unterrichtseinheit	UE 20	CNFP
	Roundup: Abschlusskapitel ✓ OSSEC (Open Source HIDS Security) ▪ Grundkomponenten ✓ Graylog ▪ Aufwand und Möglichkeiten ✓ Security Onion – Alarm per E-Mail ✓ Dienstleistungen im Bereich NSM ✓ NSM/SIEM Analyse ✓ Dienstleistung ▪ Tagessätze/Preise		

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 – 13:00 Uhr sehr gerne zur Verfügung.

Sie erreichen uns unter:

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

Ihre Ansprechpartner für das ITKwebcollege.FORENSIC

Christoph Holzheid
Anne Hirschlein
Sylvia Sonntag
Thomas Wölfel

Copyrights und Vertragsbedingungen

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