
TCSS
Trusted
Cyber
Security
Solutions
TRUSTED
CYBER
ACADEMY
TRAINING
TODAY'S LEADERS
FOR
TOMORROW'S THREATS
http://tcss.eu

Sie brauchen Cyber-Expertise

TRAINIEREN SIE MIT KERNELiOS EXPERTEN

KERNELiOS Cyber Command Knowledge Center

- Malware Reverse Engineering
- Exploit Development
- Advances Forensics
- Web Application Hacking
- 0-Day Hunting
- SIEM Expert
- OSINT and Social Media Analyst

Was ist der KERNELiOS Simulator?

KERNELiOS ist das erste Cyber Command Knowledge Center, das mithilfe eines Simulators die nächste Generation von Cyber-Experten trainiert.
Der KERNELiOS Simulator umfasst verschiedene Disziplinen aus dem Bereich Cyber-Sicherheit wie z.B. Verteidigung, Gegen-Angriff und Forensic, im Rahmen von Hands-On Sessions.
Die Studenten trainieren unter realistischen Bedingungen verschiedene Techniken „unter Feuer", also mit echten Attacken die im KERNELiOS Simulator umgesetzt werden.

Das Cyber Command Knowledge Center bildet die zukünftige Generation von Cyber-Security-Experten in der Branche aus, indem sie ihnen die Möglichkeit bieten, von Israels führenden Experten auf diesem Gebiet zu lernen, und dabei den Schwerpunkt auf die praktische Ausbildung in den verschiedenen Themenbereichen legen.

Der Lehrplan des Cyber Command Knowledge Centers umfasst eine Vielzahl von Themen, die für jeden Experten für Cyber-Sicherheit von Bedeutung sind. Die Vision der Gründer ist es, Studenten auszubilden, die später als Wissenszentrum für Cyber-Sicherheit in ihren jeweiligen Organisationen dienen werden.

TCSS
Trusted Cyber Security Solutions

Course Overview (1)

Cyber Awareness Enhancement – Management Introduction

Cyber Management Intro – 2 Days

The student will be exposed to vast abilities to comprehend cyber risks and components.
The workshop manager will be exposed to a whole range of topics and methods of defense and attack that are common in the world.
This unique workshop was developed to allow you to cope with the existing threat in our cyber world.
The subjects in this workshop were chosen in order to include most of the defensive tools and the attacks a manager can encounter in his organization on a day-to-day basis. Designed for people who want to understand the field in a broad way.

Cyber Awareness Enhancement - OSINT

Open Source Intelligence (OSINT) – 2 Days

Providing tools and knowledge of the Internet world as "the arena" and the
use of social networks as a source of information.
Knowledge of the existing sources of information, including social networks benefits that can be derived from them, how to operate in the internet without being blocked and arouse suspicion, and treatment of different
media types.

Special demand?

We will be happy to adapt all trainings to your special needs, be it concerning the content, the location or the duration. Please contact us, we will be happy to make you a quotation suitable for your individual needs

Cyber Forensics - Memory

CHWMFE- Certified Hands-On Malware Analysis and Windows Memory Forensics Expert – 5 Days

This course provides the critical skills necessary for digital forensics examiners and incident responders to successfully perform live system memory triage and analyze captured memory images.r Hands-on training courses|

Cyber Forensics – Investigative Mode

CHCFE – Certified Hands-On Cyber Forensic Expert – 5 Days

This course covers the up-to date topics in the digital forensics field. The course will describe the forensic tools, methods, techniques and what to look for when investigating a digital computer event.
You will learn how to forensically copy, analyze, recover, search and investigate artifacts in your organization in different scenes.
The course will also cover the methods to collect evidence that will be valid in court.

Web Security – Web Hunter

CHWVH - Certified Hands-On Web Vulnerability Hunter (0-day hunting) – 5 Days

The course will introduce the common techniques used when auditing massive pieces of code, teach you how to detect complex vulnerabilities, and give you the tools to exploit them.

Web Security – Hacker Mode

CHWAH - Certified Hands-On Web Application Hacker – 5 Days

The objectives of the course are to teach developers and security professionals how to find and exploit the most dangerous web vulnerabilities, giving them the tools necessary in order to audit web applications by themselves.

Course Overview (2)

Cybercrime – Malware Analysis

CHMAE – Certified Hands-On Malware Analysis Expert – 5 Days

An advanced reverse engineering course with emphasis on Windows operating system from a very experienced 8200 alumni (IDF Intelligence).Topics include research of malware, sandbox detection, code packing and unpacking, encryption and anti-debugging, exploits and a lot of low-level code!

Security and events management

CHSE – Certified Hands-On SIEM Expert – 5 Days

This course will walk you through the SIEM-SOC world with the advanced theory of SOC generations, strategies, build your own SOC, and open discussions to enrich knowledge and share new ideas between the students. Altogether with many LABs to practice event lifecycle via data mining, normalizing, handling and visualizing to better understand SIEM behind the scene.

Cyber Security - 102

CHPTE – Certified Hands-On Penetration Tester Expert – 15 Days

Intermediate cyber security course intended for students seeking to enhance their PT and Python abilities. This course is offer as next level course for our graduate of the CHCSS program.

Cyber Security - 101 Basic

CHCSS - Certified Hands-on Cyber Security Specialist – 310 Hours

Entry level cyber security course intended for an audience looking to make a career change, or alternatively for those wishing to enter the world of cyber and information security.
Students in the course will be exposed to a whole range of topics and methods of defense and attack in the cyber world and practice the material with tools that simulate what happens in the real world, tools required for the ongoing work of modern cyber security person in a changing world.

Cyber Security - 101

CHCSS - Certified Hands-on Cyber Security Specialist – 510 Hours

Entry level cyber security course intended for an audience looking to make a career change, or alternatively for those wishing to enter the world of cyber and information security.
Students in the course will be exposed to a whole range of topics and methods of defense and attack in the cyber world and practice the material with tools that simulate what happens in the real world, tools required for the ongoing work of modern cyber security person in a changing world.

Course Description

This unique workshop was developed to allow a manager to cope with the existing threats in our cyber world.

The participants will be exposed to vast techniques in order to comprehend cyber risks and components.

The managers will be exposed to a whole range of topics and methods of defense and attack that are common in the cyber world.

The subjects in this workshop were chosen in order to include most of the defensive tools a manager can encounter in his organization on a day-to-day basis in order to help him get the right decision.

Designed for people who want to understand the field in a broad way and do not require any previous cyber knowledge.

Target Audience

This course is intended for managers from all levels and also for policy decision makers in an organization.

Prerequisites

- Good knowledge of English
- Cyber or information security knowledge is not needed

Course Description

The world of the Internet is changing and growing at a faster rate from day to day and contains countless databases who collect personal data and are stored on the Web.

We upload our details to the network through social networks, forums, applications, etc., and do not aware for the vast amount of information collected about us, which is stored in the "cloud". With the right tools you can find the signal within the big noise (Internet) and find information that helps us to investigate the target of the investigation.

The course provides tools and knowledge of the Internet world as "the arena" and the use of social networks as a source of information.
Knowledge of the existing sources of information, including social networks and the benefits that can be derived from them, how to operate in the internet without being blocked and arouse suspicion, and treatment of different media types.

Target Audience

The course is intended for managers at all levels, as well as for information security workers in the organization in which they work or employees who deal in intelligence and investigations.

Prerequisites

- Good understanding of technical English
- No need for any information security knowledge

Agenda

2 Days, 10 academic hours per day (Total of 20 Academic hours)

Course Description

It is easy to get lost when auditing the code of a large, complex, application.
Sometimes, the vulnerability is there but you just don't know how to reach it, and other times it seems you just can't find anything.
This unique course will help you find your way around those complex applications, teaching you advanced exploitation techniques and giving you the tools necessary to navigate tens of thousands lines of code with ease.
The course will introduce the common techniques used when auditing massive pieces of code, teach you how to detect complex vulnerabilities, and give you the tools to exploit them.
The objective of the course is to let you feel comfortable with auditing massive projects, knowing how to detect and exploit vulnerabilities in it, so you could ultimately find your very own 0-day.

Target Audience

The course targets members of the security industry wishing to improve their white box code auditing skills.

Prerequisites

In order to gain the most out of the course, students should be familiar with:
- Web-Security exploitation techniques (SQLI, LFI/RFI, XSS)
- Experience in web development languages (PHP, Java, JS)

Course Description

The cyber forensics course covers up-to date topics in the digital forensics field. The course will describe the forensic tools, methods, techniques and what to look for when investigating a digital computer event.

You will learn how to forensically copy, analyze, recover, search and investigate artifacts in your organization in different scenes.

The course will also cover the methods to collect evidence that will be valid in court.

The course is designed to practice the students in various real-life scenarios with an emphasize on hands-on training.

Each student will have its own labs and tools for practice.

This course is a great opportunity to jump into the growing domain of digital forensic field.

Target Audience

Law enforcement and police personnel, forensics specialists, Savvy sysadmins, CISO's, Technical & seasoned persons who wants to plunge in to the digital forensics world.

Prerequisites

- Foundational understanding of Windows OS's
- Foundational understanding in the Information Security field
- Foundational understanding of core networking concepts such as TCP/IP
- Strong desire to learn the digital forensics tools and techniques

Course Description

Our web applications are under attack on a daily basis and the next security breach is just a matter of time.
This thorough hands-on course will teach you how to find and fix those security holes in your web applications before the bad guys do.
The course will introduce the various methods, tools and techniques used by attackers, in order to know how to test for the major security vulnerabilities and how to identify security bugs on real systems, by using live hacking demonstrations and hands-on labs.
The objectives of the course are to teach developers and security professionals how to find and exploit the most dangerous web vulnerabilities, giving them the tools necessary in order to audit web applications by themselves.
This course provides intensive hands-on labs featuring many real-world scenarios.

Target Audience

The course targets members of the software development industry and security professionals wishing to improve their web-security skills.

Prerequisites

In order to gain the most out of the course, students should be familiar with:
- Backend web development practices and languages (PHP, .NET, etc.)
- Basic client-side web development (HTML, JS, CSS)
- Basic databases knowledge and the SQL language

Course Description

An advanced reverse engineering course with emphasis on Windows operating system from a very experienced 8200 alumni.

Topics include research of malware, sandbox detection, code packing and unpacking, encryption and anti-debugging, exploits and a lot of low-level code!

Target Audience

This course is intended for Malware analysts, Reverse engineering experts and security professionals wishing to improve their cyber defense skills

Prerequisites

- C++ programming
- Python
- x86/x64 assembly - Optional

Course Description

SIEM-SOC course for admins, analysts, and advanced users.

this 5 day course will walk you through the SIEM-SOC world with the advanced theory of SOC generations, strategies, build your own SOC, and open discussions to enrich knowledge and share new ideas between the students. altogether with many LABs to practice event lifecycle via data mining, normalizing, handling and visualizing to better understand SIEM behind the scene.

How to get data, how to sanitize, normalize, aggregate, parse and so forth.
We will use cutting-edge SIEM and data technologies, environments and best practices to get you deep inside the process.

Target Audience

SIEM/SOC operators and managers , SIEM analysts

Prerequisites

- Knowledge in Regex
- Working with a SIEM solution
- Knowledge with ELK solution

Course Description

Intermediate cyber security course intended for students seeking to enhance their PT and Python abilities.

This course is offer as the next level course for our unique CHCSS program graduates.

Topics include working with Python, learning to use basic object-oriented programing, working with Python projects, using threads and learning coding conventions.

The second part of the course include topics of gathering cyber intelligence, learn to do penetration testing for both application and infrastructure level, using various exploitation tools and making payloads for attacks. Learn to use tools for various cyber-attacks like Wi-Fi hacking, MITM XSS, SQL Injections ,Phishing, session hijacking, etc.

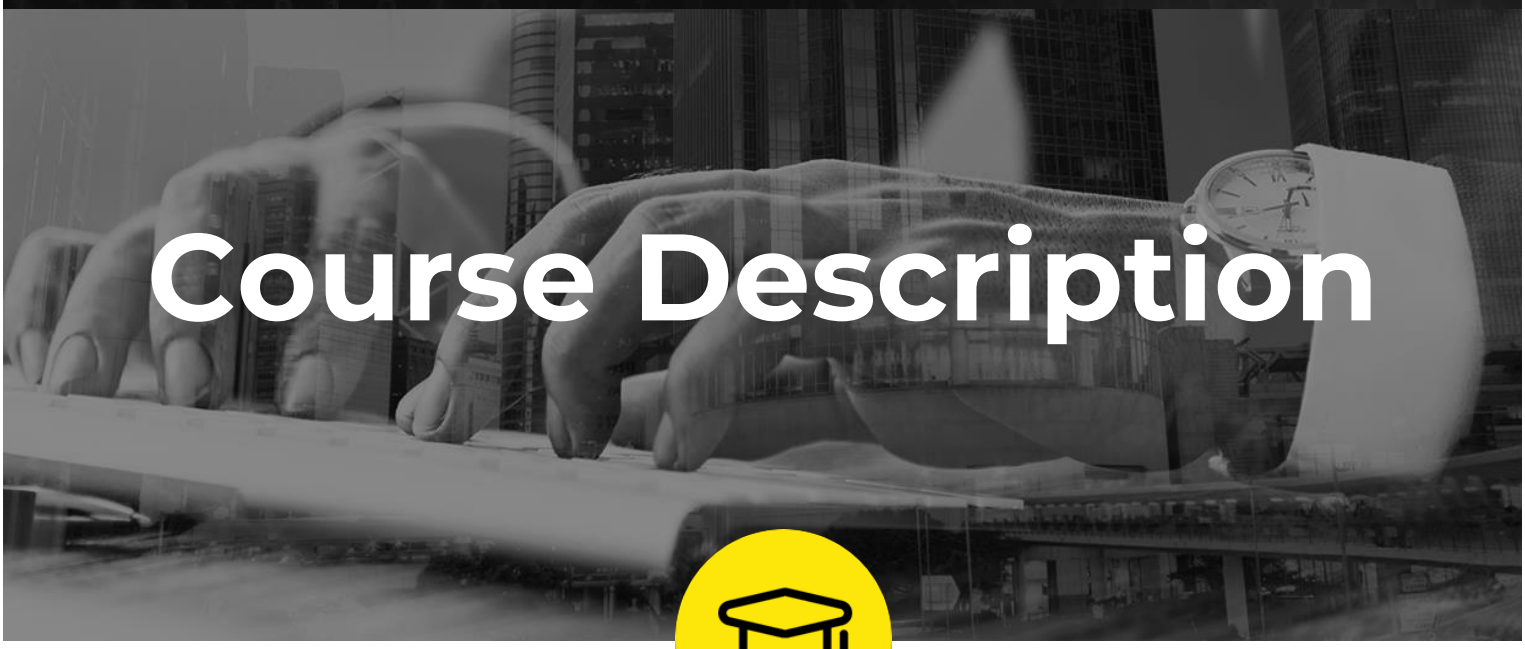
The course also gives tools for evaluate vulnerability in web sites. All of those topics are being practice by the students in our Hands-On labs that were develop specifically for the purpose of this course. The students also using our unique cyber simulator for practical knowledge on how to mitigate the various attacks. The course also contains homework for the students as additional hands-on material.

Target Audience

This course is intended for intermediate security personnel wishing to learn how to use the various tools for successful PT.

Prerequisites

- Good understanding of basic cyber-attacks and tools.
- Good understanding of networking protocols and TCP/IP
- Using Kali and basic Linux commands - Recommended



Course Description

Entry level cyber security course intended for an audience looking to make a career change, or alternatively for those wishing to enter the world of cyber and information security.

Students in this course will be exposed to a whole range of topics and methods of defense and attack in the cyber world and practice the material with tools that simulate what happens in the real world, tools required for the ongoing work of modern cyber security person in a changing world.

This unique training course is developed by the leading professionals in their field in Israel, and is comprised of a variety of topics required in the industry, with a great emphasis on imparting practical knowledge in cyber defense.

The aim of this course is to expose the student to a whole range of theories and practical tools in order to create a broad knowledge-base that will enable the student to successfully integrate into the cyber industry.

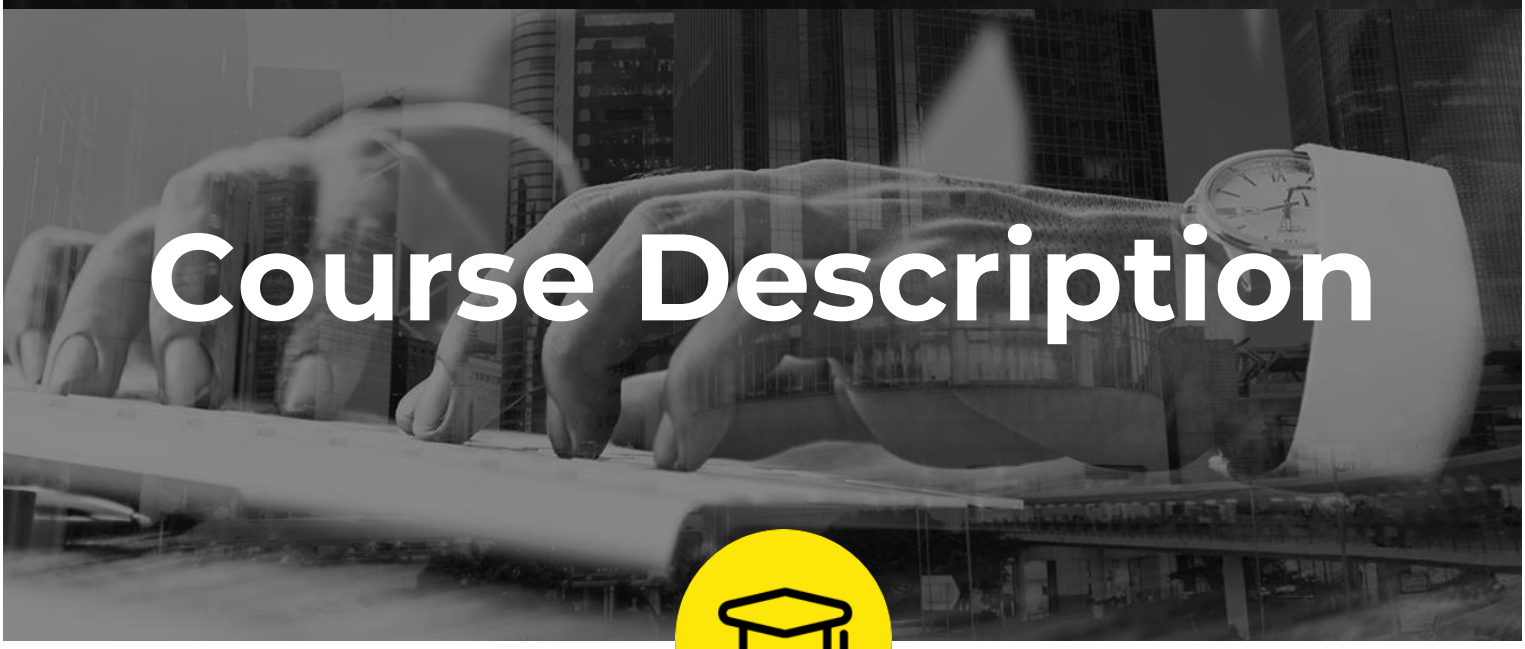
The course also contains homework for the students as additional material.

Target Audience

This course is intended for anyone wishing to learn cyber security and enter the cyber world.

Prerequisites

- Good understanding of basic Windows environments
- Technical level of English reading



Course Description

Entry level cyber security course intended for an audience looking to make a career change, or alternatively for those wishing to enter the world of cyber and information security.

Students in this course will be exposed to a whole range of topics and methods of defense and attack in the cyber world and practice the material with tools that simulate what happens in the real world, tools required for the ongoing work of modern cyber security person in a changing world.

This unique training course is developed by the leading professionals in their field in Israel, and is comprised of a variety of topics required in the industry, with a great emphasis on imparting practical knowledge in cyber defense.

The aim of this course is to expose the student to a whole range of theories and practical tools in order to create a broad knowledgebase that will enable the student to successfully integrate into the cyber industry.
The course also contains homework for the students as additional material.

Target Audience

This course is intended for anyone wishing to learn cyber security and enter the cyber world.

Prerequisites

- Good understanding of basic Windows environments
- Technical level of English reading

Kontakt

Österreich

Trusted Cyber Security Solutions GmbH
Tuchlauben 7a
A-1010 Wien, Austria
Phone: +43 664 8103110
e-mail: office@tcss.eu

Deutschland

Trusted Cyber Security Solutions GmbH
Winterhuder Weg 29
D-22085 Hamburg, Germany
Phone: +49 176 63152514
e-mail: office@tcss.eu