CYBER SECURITY SKILLS TRAINING PROSPECTUS

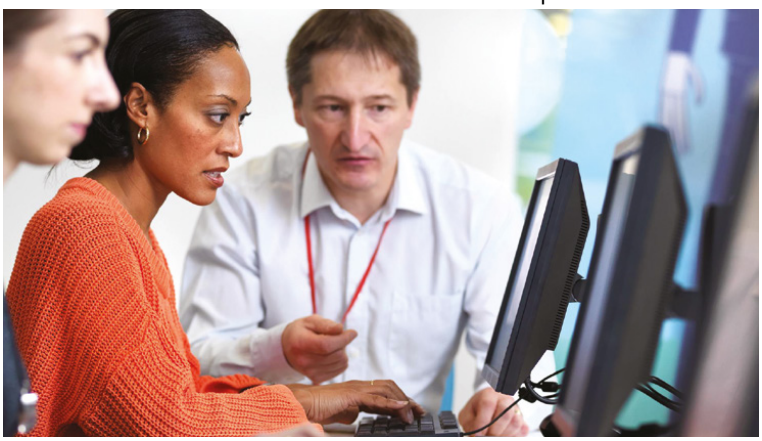
PA Consulting Services Ltd, Global Innovation and Technology Centre, Melbourn, Herts, SG8 6DP, United Kingdom
tel: +44(0) 1763 285 285 email: cybereducation@paconsulting.com web: cybereducation.paconsulting.com

CYBER SECURITY SKILLS TRAINING PROSPECTUS

CONTENTS

Cyber skills training at PA

Cyber Security and Digital Investigations are rapid growth areas within IT and the skills required are in demand.



Why train with PA

1. Our courses are **taught by our practicing consultants** who bring their experience directly to the classroom.
2. We offer a **work-based approach** to our training, with hands-on exercises enabling you to transfer your skills to the workplace.
3. Our courses are **developed, delivered and regularly revised** to reflect the latest developments, techniques, exploits and defensive recommendations - an approach that guarantees up-to-date and highly relevant real-world content.
4. You will become a **recognised cyber professional** on achieving the course certification.
5. Our technical training courses provide **industry-recognised certifications**.

Training Passports

Discounted training with our Training Passports are the most economical way to get all the training that you or your team needs.
Each Training Passport enables you to purchase a set number of training days – which can be used across our entire portfolio of public-scheduled courses – for a discounted rate compared to when booking the courses individually.

On-site Training

For groups of 8 people or more, we can deliver our courses or a bespoke tailor-made programme delivered on at your premises. This is well-suited to those clients who wish to have personalised content and delivery to enhance the business benefits for their delegates.

Benefits:

- Train more of your team
- Improves flexibility by arranging training to suit your business and schedule
- Significantly reduces your overall training costs, saving on travel, accommodation and subsistence

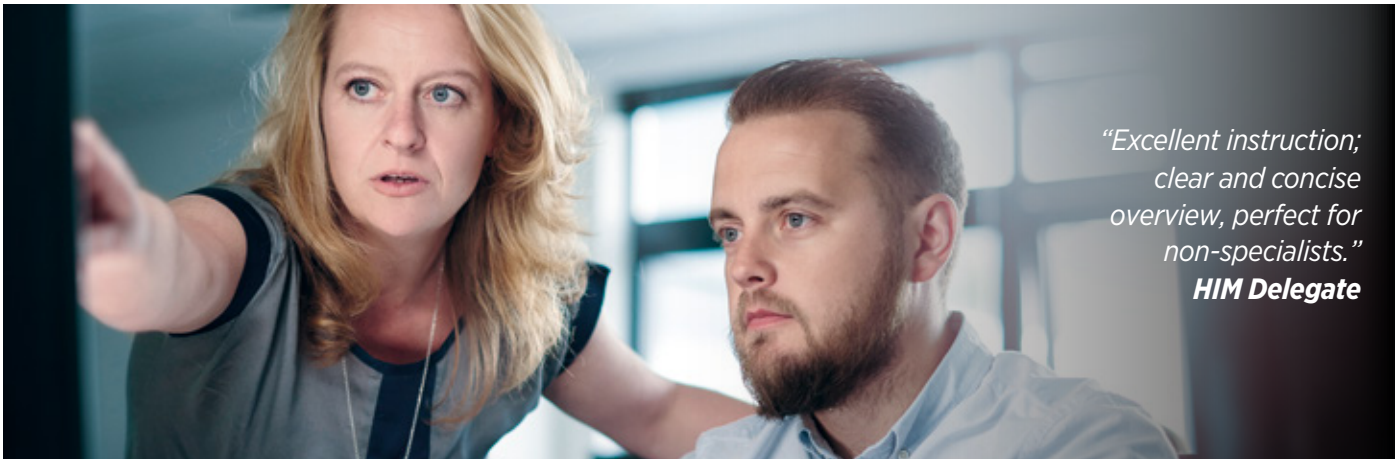
Cyber Development Skills Overview

See the Table below for an overview of our public course programme, which shows the full range of our cyber skills courses and the study level for each.

	Awareness	Fundamentals	Core	Specialist
ETHICAL HACKING • Penetration Testers/Ethical Hackers • IT Security Managers • Software & Application Developers • Cloud Architects • System administrators and architects	**HIM** Hacking insight for managers		**CSTA** Ethical Hacking **CSTP** Ethical Web Hacking **CCSA** Cloud Security	
DIGITAL FORENSICS • Computer Forensics Consultants • Cyber Security Analysts • Data Forensics Technicians • Forensic Computer Analysts		**CDaCT** Data Acquisition	**CFIP** Forensic Investigation **CMI** Malware Investigation **CCDI** Corporate Digital Investigation	**CFIS** Forensic Investigation **CCI** Network Forensic Investigation **CLFP** Linux Forensic Investigation **CMIP** Malware Investigation
INFORMATION SECURITY • Finance, IT, sales & HR teams • IT Security Officers & Auditors • Information security professionals		**CIIP** ISO 27001 Implementation		
INCIDENT RESPONSE • Cyber Security Incident Responders • Security Operation Centre Analysts • Threat Hunters	**CSIRM** Cyber Security Incident for Managers	**CSOCA** Security Operation Centre functions		**CSIR** Cyber Security Incident Response **CCTH** Certified Cyber Threat Hunting

ETHICAL HACKING COURSES AND CERTIFICATIONS OVERVIEW

Our ethical hacking courses are aimed at penetration testers, software developers, system administrators and network architects. We provide the latest techniques as well as valuable insight into the attack methods used by hackers and how to defend your systems against them. Our courses are between one and five days of hands-on experience, using practical exercises to discover and learn techniques/ methods that will provide both developing and experienced cyber professionals with the latest in-depth knowledge.



ETHICAL HACKING
Hacking Insight for Managers (HIM)

●○○○ **AWARENESS-LEVEL COURSE**

This one-day awareness course is for people who need a high-level understanding of hacking rather than practical know-how. It introduces the basic technical concepts behind the various stages of a hacking attack, as well as some common tools used by hackers and security professionals.

What will I learn?

- You will gain an insight into the mindset and motivation of hackers, and learn how they infiltrate organisations and the damage that can follow
- You will find out how organisations are exposed through the various routes of attack, including the internet, employees, social engineering, emails and wireless
- You will learn about the security lapses behind a number of real-world, high-profile attacks
- You will have the chance to try your hand at some simple web application attacks in our 'hack lab'

How will I benefit?

On this course, you will:

- Gain an understanding of IT security from an attacker's perspective
- Be able to evaluate the possible risks to your business from hackers
- Understand the principles of how to defend your organisation effectively from the risk of attack

Who should attend?

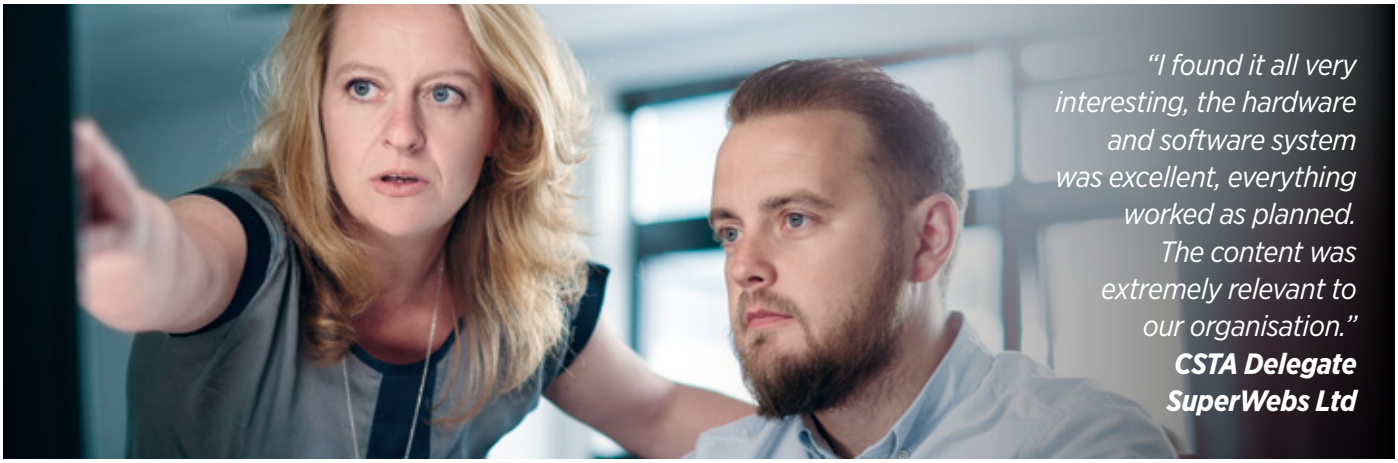
Anyone interested in understanding the risks that hackers pose, including:

- IT managers
- Systems analysts
- IT security professionals and auditors
- Security officers and data protection representatives

For a course with more hands-on technical content, delegates should consider our CSTA and CSTP courses on pages 7 and 8.

HIM prerequisites

- No information security knowledge is needed, just basic computer literacy
- We recommend you read up on the concept of domain names and IP addresses before the course
- Bring a Wi-Fi enabled device to join the 'hack lab' (e.g. laptop or tablet)



ETHICAL HACKING
Certified Security Testing Associate (CSTA)

●●●○ **CORE-LEVEL COURSE**

This infrastructure ethical hacking course is our most popular core-level technical course for people from a wide variety of network related and security roles across all industry sectors looking to develop their own capability to support their organisation's in-house cyber team.

What will I learn?

- You will learn a series of attack methodologies and gain practical experience using a range of tools to undertake an infrastructure penetration test across a multi-OS environment
- Once you are able to identify and exploit vulnerabilities in a safe manner, you will be introduced to a range of defensive countermeasures, allowing you to protect your network and respond to cyber threats

How will I benefit?

This course in particular will give you:

- Valuable preparation and hands-on practice in preparation for the CREST Registered Penetration Tester (CRT) examination
- Understanding of common infrastructure vulnerabilities and how to exploit or resolve them

What qualification will I receive?

Upon successful completion of the exam, you will be awarded the Certified Security Testing Associate (CSTA) qualification, accredited by both CREST and the IISP.

Who should attend?

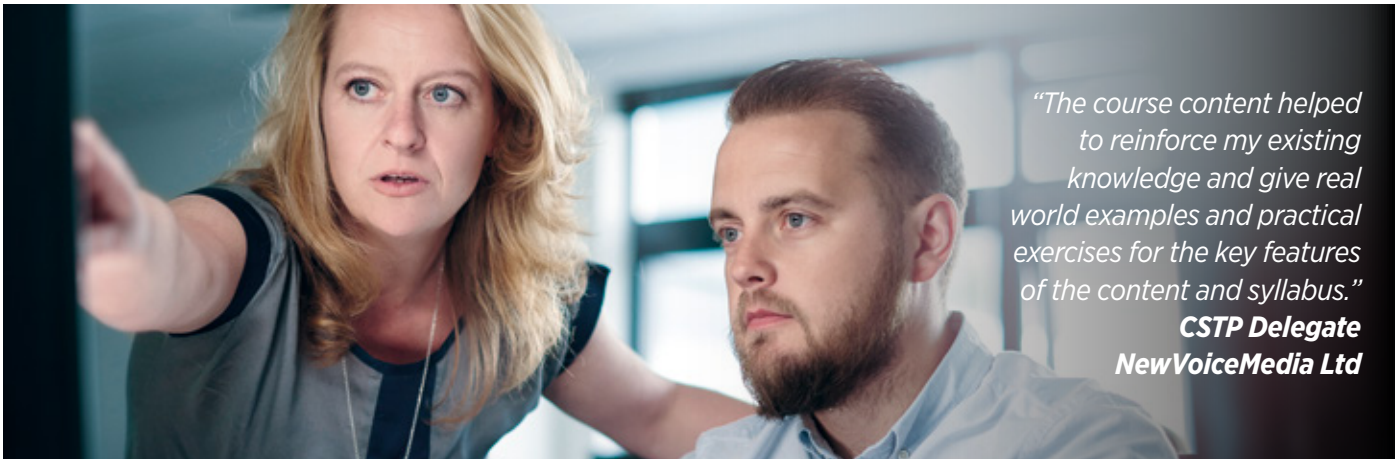
If you are looking to improve your career prospects by starting or transitioning into a cyber security role e.g.

- Network engineers
- Systems administrators
- Systems architects or developers

CSTA prerequisites:

Basic understanding of TCP/IP networking and comfortable with Windows and Linux command line.

CSTA is also a good source of information on TCP/IP networking, should you wish to refresh your knowledge.



ETHICAL HACKING
Certified Security Testing Professional (CSTP)

●●●○ **CORE-LEVEL COURSE**

This web application ethical hacking course is designed to give you the skills you need to ensure valuable data assets are effectively protected.

What will I learn?

- You will be introduced to a range of defensive countermeasures to become more resistant to attack
- You will learn how to exploit these vulnerabilities to access data and functionality beyond your remit

How will I benefit?

This course will give you:

- Valuable preparation for the CREST Registered Penetration Tester (CRT) examination and the knowledge required to join our CAST course (advanced web application security)
- The skills and understanding to progress to the next stage in your career as a security professional

What qualification will I receive?

Upon successful completion of the exam, you will be awarded the Certified Security Testing Professional (CSTP) qualification.

Who should attend?

Anyone with responsibility for, or an interest in, the security of web applications, including:

- System administrators
- Software developers
- Budding penetration testers
- Anyone subject to the requirements of the Payment Card Industry Data Security Standard (PCI DSS)

CSTP prerequisites

An understanding of how a web page is requested and delivered:

- Are you familiar with the high-level components involved, e.g. browsers, web servers, web applications and databases?
- What are HTTP and HTML?
- An understanding of databases and SQL would also be an advantage

"Very interesting content covering the top three public cloud providers and underpinned by good practical examples across the spectrum. With Public Cloud Security being such an important topic the course is well worth attending"
CCSA Delegate

COURSE OUTLINE

ETHICAL HACKING
Certified Cloud Security Analyst (CCSA)

●●●○ **CORE-LEVEL COURSE**

Adoption of public cloud services is now more popular than ever. This course will help you understand the common weakness across the three most popular public cloud providers as well as arm you with the skills necessary to audit a cloud environment against industry recognised best practises. This course mixes practical examples of misconfiguration with both manual and automated audit techniques.

THE SKILLS YOU WILL LEARN

- The core functions and differences of the top three cloud providers
- Examples and practical demonstrations of "attacks against the cloud"
- Weaknesses and common misconfigurations of cloud services
- Best practices for securing cloud environments
- Practical enumeration of public weaknesses

KEY BENEFITS

This course will enable you to:

- Identify weaknesses in cloud environments
- Help design more secure solutions
- Prevent unauthorised users gaining access to public resources
- Gain the ability to identify weaknesses before they become vulnerabilities

WHO SHOULD ATTEND

Anyone with responsibility for, or an interest in, the security of cloud environments, including:

- Cloud architects
- System administrators
- Penetration testers

PREREQUISITES

An understanding of how public cloud works and general web architecture:

- Familiarity with general networking and computing concepts
- Command line and API usage and concepts

An understanding of virtualisation, technologies surrounding shared computing resources and remote access would also be beneficial.

WHAT QUALIFICATION WILL I RECEIVE?

Those delegates successfully passing the exam at the end of the course will be awarded the Certified Cloud Security Analyst (CCSA) qualification.

DIGITAL FORENSICS COURSES AND CERTIFICATIONS OVERVIEW

We have successfully delivered our certified digital forensic training courses to numerous law enforcement and legal professionals as well as private corporations across all industry sectors. Our programme is aimed at forensic investigators, digital security practitioners and those with computer forensic experience wanting to develop skills further in order to conduct thorough, efficient and comprehensive investigations. Expert trainers and practical technical exercises will ensure you have the latest industry best practice knowledge and tools to conduct the most effective digital forensic investigations for your organisation.

"Steve Shepherd MBE has a great personality for teaching and has the ability to make the course fun and interesting. I have thoroughly enjoyed the course and will be sending my team on it."
CDaCT Delegate
City Docs Ltd

DIGITAL FORENSICS
Certified Data Collection Technician (CDaCT)

●●○○ **FUNDAMENTALS-LEVEL COURSE**

This is a fundamentals-level course for people who have to handle or advise on electronic evidence/ data on a regular basis and provides them with the skills to ensure that forensic and evidential integrity is retained when data is transferred or copied.

What will I learn?

- You will be introduced to the legalities, best practice and current techniques used for data acquisition as part of forensic investigation, eDiscovery or other regulatory proceedings
- You will carry out forensic imaging in a number of environments, using different methods and software
- You will learn how to extract individual mailboxes from a live Microsoft Exchange email server, as well as live system memory and volatile data capture

How will I benefit?

This course will give you:

- The skills you need to be competent in handling data during the initial stages of investigation
- The opportunity to practice identifying and collecting electronic evidence/ data and build your confidence
- An industry-recognised qualification in data collection

What qualification will I receive?

Upon successful completion of the exam, you will be awarded the Certified Data Collection Technician (CDaCT) qualification.

Who should attend?

Anyone responsible for the process of data acquisition, including:

- Law enforcement officers and agents
- Network administrators
- IT security officers
- Civil litigation lawyers/legal council
- Litigation support managers
- eDiscovery consultants

CDaCT prerequisites

A general appreciation of information technology and computer forensic principles/methods is desirable, but not essential.

DIGITAL FORENSICS
Certified Forensic Investigation Practitioner (CFIP)

●●●○ **CORE-LEVEL COURSE**

This core-level technical course is designed for people looking to develop their computer forensics investigation skills, either for a career in digital investigations or as part of their current cyber role.

What will I learn?

- You will learn the principles and guidelines for static computer forensic investigations; the fundamentals of the complete forensic investigation process; how to preserve evidence and the methodology for conducting a forensic investigation
- You will use practical, hands-on exercises to help you understand how data is stored on electronic media, how to work with key forensic investigation tools and how to identify Windows-based OS forensic artefacts

How will I benefit?

The course will give you:

- An understanding of each stage of a forensic investigation, from evidence seizure through to data investigation and interpretation, to report and presentation of findings
- The skills to allow you to undertake the forensic acquisition of an electronic device
- Confidence in working with key forensic investigation products
- An industry-recognised qualification in forensic investigation and ideal preparation for the CFIS advanced course

What qualification will I receive?

Upon successful completion of the exam, you will be awarded the Certified Forensic Investigation Practitioner (CFIP) qualification.

Who should attend?

Anyone who is or wants to be responsible for computer forensic investigations, including:

- Cyber forensic and network investigators
- IT security officers
- Law enforcement officials

CFIP prerequisites

Experience with Microsoft Windows OS and, ideally, a general appreciation of forensic principles, practices and software.

DIGITAL FORENSICS
Certified Malware Investigator (CMI)

●●●○ **CORE-LEVEL COURSE**

This is a core-level technical course for people looking to extend their digital forensic knowledge beyond conventional device analysis. It will help you protect your IT environment by showing you how to conduct malware analysis, from first principles all the way to investigating network activity stemming from malicious software infection that your AV software has failed to detect.

What will I learn?

- You will learn how to identify, analyse and interpret malicious software and associated forensic artefacts, including trojan horses, viruses and worms
- You will practice malware investigations from mounted, booted and network perspectives, and undertake real-world exercises, including the conversion of E01 forensic images to bootable virtual machine disks

How will I benefit?

The course will give you:

- The skills to analyse and interpret malicious software, and investigate network activity initiated by malicious software infection
- An understanding of how to simplify complex evidence, and collate and report results
- An industry-recognised qualification in malware investigation

Who should attend?

Digital forensic analysts, law enforcement officers, cyber incident investigators and system administrators looking to develop their skills in malware identification and analysis.

CMI prerequisites

Completion of the CFIP course is highly recommended. Otherwise you will need:

- Knowledge of the principles surrounding forensic investigation and an understanding of the preliminary forensic investigation case considerations
- Sound experience with the Microsoft Windows operating systems
- An understanding of how a web page is requested and delivered
- Ideally an understanding of Command Line Interface (CLI) and TCP/IP networking concepts

What qualification will I receive?

Upon successful completion of the exam, you will be awarded the Certified Malware Investigator (CMI) qualification.

DIGITAL FORENSICS
Certified Linux Forensic Practitioner (CLFP)

●●●● **SPECIALIST-LEVEL COURSE**

This specialist-level course is for experienced forensic investigators who want to acquire the knowledge and skills to navigate, identify, capture and examine data from Linux-based systems.

What will I learn?

- You will develop a core understanding of the file system data structures and key files in Linux-based systems so that you can be confident of capturing potential digital evidence
- You will practice using both Linux GUI and command line environments, and learn how to use Linux for forensic imaging
- You will capture RAM and basic volatile data from a live Linux system, and use forensic software to create an image of a Linux system

How will I benefit?

On this course, you will:

- Understand the data structures associated with the 'ext' file systems
- Learn effective techniques to identify and collect data from a Linux environment
- Develop confidence when faced with a Linux system
- Improve your ability to respond effectively to a wider range of forensic incidents

What qualification will I receive?

Upon successful completion of the exam, you will be awarded the Certified Linux Forensic Practitioner (CLFP) qualification.

Who should attend?

Forensic practitioners, systems administrators and cyber investigators who want to extend their experience from Window-based systems to the Linux environment.

CLFP prerequisites

Completion of the CFIP course is highly recommended. Alternatively you will need an understanding of digital forensic principles and practices. No Linux experience is necessary.

DIGITAL FORENSICS
Certified Forensic Investigation Specialist (CFIS)

●●●● **SPECIALIST-LEVEL COURSE**

This specialist-level course is for professionals whose role requires them to capture and analyse data from 'live' systems.
It introduces the latest guidelines and artefacts on current Windows operating systems, and teaches essential skills for conducting an efficient and comprehensive investigation.

What will I learn?

- You will learn to capture volatile and stored data from a system in a 'live' and 'booted' state and from remote and virtualised systems, and to capture mailboxes from a Microsoft Exchange Server and webmail accounts
- You will practice your new skills using a realistic data/IP theft scenario employing a range of forensic tools, scripts and techniques. You will identify data from the Windows domain controller, network file shares and FTP logs before moving to more conventional analysis of a forensic image of a workstation

How will I benefit?

This course will enable you to:

- Develop your forensic investigation skills to an advanced level
- Practise new techniques suitable for evidence identification, capture and analysis in a 'live' environment
- Acquire an industry-recognised qualification to support your career progress

What qualification will I receive?

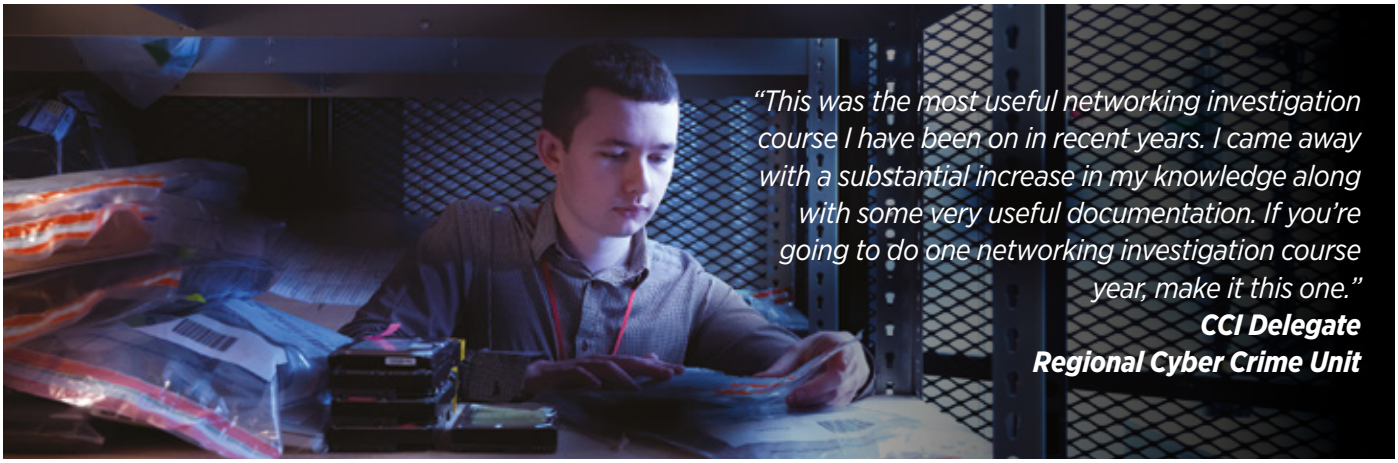
Upon successful completion of the exam, you will be awarded the Certified Forensic Investigation Specialist (CFIS) qualification.

Who should attend?

Experienced forensic investigators and digital security practitioners who have computer forensic experience who want to dig deeper and develop their skills. This course is a natural progression from the CFIP course.

CFIS prerequisites

- Knowledge of the principles and general guidelines surrounding forensic investigations
- Experience of carrying out forensic investigations
- Attendance of a basic computer forensic course, e.g. PA's CFIP course



DIGITAL FORENSICS
Certified Cyber Investigator (CCI)

●●●● **SPECIALIST-LEVEL COURSE**

This specialist-level course is for professionals who are looking to develop and improve their ability to respond effectively to a cyber event. It helps you develop the skills needed to isolate, investigate and extract evidence from a live networked environment during or after a cyber incident.

What will I learn?

- You will learn and practice the critical skills needed to identify the correct forensic artefacts in a live network environment during or after a cyber event, and how to preserve and collect that data
- You will practice how to correctly acquire and handle dynamic data so that you do not inadvertently alter or destroy vital clues that could result in your investigation failing or the resultant evidence being inadmissible in court

How will I benefit?

This course will enable you to:

- Learn a number of methodologies for undertaking a sound cyber investigation
- Acquire and practice new techniques to extract relevant data from a live networked environment
- Gain confidence when identifying and capturing live operating system artefacts
- Improve your ability to respond effectively to a cyber event

What qualification will I receive?

Upon successful completion of the exam, you will be awarded the Certified Cyber Investigator (CCI) qualification.

Who should attend?

Experienced forensic investigators and cyber security practitioners who already have a good knowledge of forensic investigation and want to extend their skills.

CCI prerequisites

You will need a good understanding and experience of:

- The forensic investigation process
- Windows and Linux operating systems
- Command line interface
- Computer networks

We strongly recommend completion of the CFIP and CLFP courses as a minimum before attending this course.

DIGITAL FORENSICS Certified Malware Investigation Professional (CMIP)

SPECIALIST-LEVEL COURSE

This is a specialist-level technical course for people looking to extend their knowledge beyond the basics of malware investigations. This course builds on the core foundations of our Certified Malware Investigator (CMI) course and will give delegates a deeper technical understanding of how to investigate a suspected malware infection.

What will I learn?

You will learn how to identify artefacts consistent with complex malware
- Understand how malware can obfuscate itself and hide in plain sight
- Practice malware investigations in a live environment
- Investigate Random Access Memory
- Understand structures of key NT file system metadata files

Practical application of course content will be through case scenarios in order to understand how complex malware functions within a Windows environment.

How will I benefit?

The course will give you:
- The skills to understand and interpret malware within a Windows environment
- Practical experience of investigating Random Access Memory

Who should attend?

For those looking to further develop their skills in malware investigations, including:
- Digital forensic practitioners
- Cyber security responders
- Security operations specialists

CMI prerequisites

You will need an understanding and experience of:
- Investigating malware infections
- Windows 10 Operating Systems
- The NT File System
- Memory Analysis
- PowerShell and other command line tools

We strongly recommend completion of the PA Certified Forensic Investigation Specialist (CFIS) and Certified Malware Investigator (CMI) courses as a minimum before attending.

What qualification will I receive?

Upon successful completion of the exam, you will be awarded the Certified Malware Investigation Professional (CMIP) qualification.

DIGITAL FORENSICS
Certified Corporate Digital Investigator (CCDI)

●●●○ **CORE-LEVEL COURSE**

This is a core-level course designed for corporate investigators who are required to identify, secure or recover electronic evidence. It has been developed for investigators based in both the private and public sectors, to ensure that the forensic and evidential integrity is controlled and accounted for during the data recovery process.

How will I benefit?

This course will give you:

- The skills to be competent in identifying, securing, collecting and handling data during the initial stages of an investigation
- The opportunity to practice identifying and collecting electronic evidence
- Learn methodologies that will enable you to comply with International Standards for the identification, collection, acquisition and preservation of digital evidence as described in ISO 27037
- Delegates will acquire data from different environments in numerous practical exercises to reinforce understanding and technique
- Develop skills and an understanding of policies and practices required to withstand third party scrutiny
- Gain confidence in forensic imaging and copying data from a number of different environments
- An industry-recognised qualification in data collection

INFORMATION SECURITY TRAINING COURSES AND CERTIFICATIONS OVERVIEW

Our information security courses are focused towards anyone with responsibility for, or with an interest in, protecting an organisation's IT systems & data, including those employed in IT, Business, Financial and HR Management.

INFORMATION SECURITY
Certified ISO 27001 Implementation Practitioner (CIIP)

●●○○ **FUNDAMENTALS-LEVEL COURSE**

This three-day practical ISO 27001 training course is for people who want to understand the component parts of the ISO Standard with a view to setting up an implementation project. You will learn how to define and risk-assess your organisation's information assets, and prepare for the essential requirements needed to obtain ISO 27001 certification.

What will I learn?

- You will gain an understanding of the key steps involved in planning, implementing and maintaining an ISO 27001-compliant information security management system (ISMS)
- You will learn what an ISMS is and how to define information security policies for your organisation
- You will gain the skills needed to identify information assets and undertake a risk assessment, and will acquire effective techniques for managing risk

How will I benefit?

With this course, you will:

- Gain an in-depth understanding of information security and how it applies to your organisation
- Learn how to define information assets in a way that's suitable for your organisation and how to undertake a risk assessment
- Gain confidence that certification is within reach and obtain guidance on applying for certification

What qualification will I receive?

Upon successful completion of the exam, you will be awarded the Certified ISO 27001 Implementation Practitioner (CIIP) qualification.

Who should attend?

Anyone with responsibility for, or with an interest in, information security, including:

- People employed in IT, financial and HR management
- Computer auditors
- IT security officers
- Information security professionals

CIIP prerequisites

This course is suitable for non-technical staff and no prior knowledge is required.

Managing Insider Risk

Course

September 2022

Bringing Ingenuity to Life.
paconsulting.com

SPECIALIST-LEVEL COURSE

This course will give you valuable insight into one of the major security challenges facing modern digital organisations whatever their sector. We will highlight how users can both maliciously and accidentally cause a range of harms to your organisation and how you can build the frameworks to limit such risk.

What will I learn?

• The different type of insider and how your organisation can be harmed.

• Approaches to understanding insider's motivations and behaviour prior to causing harm.

• We will share a practical risk-based approach to access your own organisation's insider risk profile. This will be brought to life in exercises.

• We will provide an overview of the key components of a successful insider risk programme.

• Trainers will also share how to avoid common pitfalls and the challenges when starting to manage this unique risk type.

Pre-requisites

No formal prior knowledge is required but you would benefit from having a working knowledge of information security and operational risk.

How will I benefit?

The course in particular will give you:

• The skills and insight to be able to understand and articulate the level of insider risk your organisation faces.

• Information needed to be able to gain support for establishing a Managing Insider Risk programme and how to structure its implementation.

Who should attend?

• Anyone with an interest or responsibility to manage both cyber and people risks in an organisation.

• It would particularly suit information and physical security managers and those in compliance and conduct functions, as well as HR managers.

INCIDENT RESPONSE & SOC TRAINING

These training courses are for professionals who are looking to develop or improve their knowledge and ability in the fields of Cyber Security Incident Response (CSIR) and SOC environments, reinforcing through practice new information and methodologies.

Our CSIR courses are aligned with the CREST Intrusion Analysis and Incident Response Syllabus, which identifies at a high-level the technical skills and knowledge that CREST expects candidates to possess for the Certification examinations in the area of Intrusion Analysis.

INCIDENT RESPONSE
Cyber Security Incident Response for Managers (CSIRM)

●○○○ **AWARENESS-LEVEL COURSE**

This awareness-level course is for those individuals involved in the decision making process or management of a cyber event involving an attack or data breach of a computer network. This course will introduce the concepts and stages to be considered during the planning and response phases to a cyber event.

Course Overview

Assuming a basic knowledge and understanding of your organisation's incident response plan, this course is ideally suited to those responsible for decision making, management planning or responding to a cyber event involving an attack or breach of a computer network. The course will detail how effective the response plan is with regard to a real-world attack or data breach

How will I benefit?

This course will give you:

- An understanding of the importance of an effective incident response plan
- The ability to appreciate and evaluate risks to your organisations data based on your incident response plan
- An understanding of the principles of preparing and responding to a cyber event

What will I learn?

- You will understand the importance of cyber security frameworks
- You will gain insight why an effective and robust incident response plan is necessary in today's interconnected world
- You will find out how organisations become exposed to certain attacks or breaches and what can be done to mitigate this
- You will learn about employee security lapses and the importance of education programmes
- You will have the chance of stopping a ransomware attack and understand some of the methods such malware uses to obfuscate and prevent removal

Who should attend?

- Anyone involved in any management aspect of preparing for or managing a cyber security event

For a course with more hands-on technical content, delegates should consider the CSIR course.

Course prerequisites:

- No CSIR technical knowledge is needed but an understanding of the requirements for information security is essential
- We recommend you refresh your knowledge and understanding of your organisations incident response plan

INCIDENT RESPONSE
Certified Security Operations Centre Analyst (CSOCA)

●●○○ **FUNDAMENTALS-LEVEL COURSE**

This fundamentals-level course provides the basic skills and knowledge for individuals who are looking to be or are currently employed within a private or public sector Security Operations Centre (SOC).

Course overview

This five-day course will enable you to understand how a SOC functions and provide you with the fundamental knowledge and understanding required for employment within a SOC. You will spend a good portion of the course is practicing and honing key skills and methodologies which replicate real-life security threat scenarios faced by SOC's today.

The skills you will learn

You will learn and practice core level and advanced skills to be an effective SOC analyst or team member.

Upon completion of the course you will have learnt:

- The threats and risks to a business network
- Gain a better understanding of threat intelligence using OSINT
- How malicious software can compromise a system
- Using SIEM tools to collate and analyse data of interest
- Fundamental and in-depth logging Analytical techniques

Key benefits

This course will enable you to gain confidence within a SOC environment by reinforcing or learning new information and methodologies.

Who should attend?

This course was specifically designed for individuals who intend to be or have recently joined as a SOC analyst or team member or to recognise those more seasoned individuals employed within the SOC.

Syllabus

Throughout the course your time will be split between being taught the methods and principles of working within a SOC and applying these in practical, hands-on exercises based on real-life scenarios.

Prerequisites

You will need a basic understanding of IT infrastructure.

What qualification will I receive?

Upon successful completion you will be awarded the Certified Security Operations Centre Analyst (CSOCA) qualification

INCIDENT RESPONSE
Cyber Security Incident Response (CSIR)

SPECIALIST-LEVEL COURSE

This specialist-level course is for technical professionals who are looking to develop or improve their knowledge or ability in the Cyber Security Incident Response (CSIR) field.

Course overview

This five-day course follows the CREST incident response model and focuses on the knowledge and key skills required to effectively respond to a cyber incident.

The skills you will learn

You will learn and practice core level and advanced CSIR skills, including:

- Advanced use of PowerShell and exploitation of WMI
- Writing of bespoke PowerShell scripts and parsers
- Identification of suspect processes
- Advanced detection and analysis of injected processes
- Identification and analysis of infected documents (MS Office & PDF) Infection vector analysis
- Rebuilding network traffic
- Breakdown and examination of log files

Key benefits

This course will enable you to learn new methodologies for responding to CSIR events and practice both core and advanced techniques. You will also gain confidence and improve your CSIR skills for when responding to a cyber event.

Who should attend?

This is an intensive training course designed for CSIR practitioners and cyber security practitioners involved in the discipline or forensic practitioners who wish to extend their knowledge and skills in this unique field. These include:

- Cyber security incident response team members
- System/network administrators/ engineers
- IT security personnel/security officers Forensic practitioners
- Law enforcement officers & agents

Prerequisites

You will need an understanding or experience of:

- The CSIR process
- Forensic investigations
- Windows operating system
- CLI

We strongly recommend completion of the CFIP and CMI courses or similar as a minimum before attending this course.

INCIDENT RESPONSE
Certified Cyber Threat Hunter (CCTH)

SPECIALIST-LEVEL COURSE

This is a specialist-level course is for those security professionals involved in penetration testing, incident response, security analysis looking to develop in their role and others wishing to enhance their proactive skills in detecting and mitigating threats.

What will I learn?

You will learn and practice the skills and understanding needed to conduct a thorough threat hunt within a live enterprise environment.

Upon completion of the course you will have learnt:

- How to correlate and analyse data to successfully identify active and passive threats already existing within a network
- How to effectively conduct and automate data collection from remote locations using built-in and third party tools so that vital clues and potential threats will not be missed

How will I benefit?

This course will give you:

- The skills to undertake your own threat hunts and develop your methodologies
- The ability to understand and correlate separate artefacts into larger patterns to better identify potential threats

What qualification will I receive?

Upon successful completion of the exam, you will be awarded the Certified Cyber Threat Hunter qualification.

Who should attend?

Experienced cyber security incident responders, SOC and security analysts and penetration testers looking to enhance their skillsets or better understand the footprints their activities may leave behind.

Course prerequisites:

This is not a beginner's course. Delegates wishing to attend should have a good working knowledge of the incident response process, requirements and technical methods used. Fundamentals of penetration testing and attack techniques, basic understanding of network nodes, traffic and host-based artefacts are also a prerequisite.

NOTES

PA Consulting Services Ltd
Global Innovation and Technology Centre
Melbourn, Herts, SG8 6DP United Kingdom
tel: +44(0) 1763 285 285
email: cybereducation@paconsulting.com
web: cybereducation.paconsulting.com