We look forward to partnering with you to combat the growing cyber threat across all industry sectors, through the delivery of the highest quality cyber security training.

Richard Allen, Education Business Development Manager
Cyber skills training at 7Safe

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

7Safe training is intensive
Our consultants coach individual delegates so that they leave with the confidence to do the job that they are training for. Our aim is to foster and develop skilled professionals capable of undertaking demanding work in the fields of penetration testing/ethical hacking, cyber security incident response, cyber threat hunting, security code review, and digital forensic investigation.

7Safe training passports
Discounted training with 7Safe’s 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 courses – for a discounted rate compared to when booking the courses individually.

On-site training:
For groups of 8 people or more, we can design a tailor-made package to meet your cyber skills requirements delivered on your site. For more details, see www.7safe.com/enterprise-training

Accredited training partners
7Safe Accredited Training Partners (ATP) based in USA, Ireland and Cyprus, offer access to our market leading cyber training programmes outside the UK.

Our training locations
7Safe offers you a wide choice of venues designed to suit your needs and budget, starting with our flagship training centre close to the vibrant City of Cambridge.

The opportunity to perform ‘hands-on’ hacking and forensic work using the latest equipment is one...
feature of our Cyber Training Programme; others are:
• Up-to-date technology and training rooms
• Free lunch and coffees throughout your course
• Air-conditioned training rooms in well-lit, spacious surroundings
• Free on-site car parking with no restrictions for private car users
• Near to major road network (M11/A10/A505) and train stations
• Only 36 minutes by train from central London*

7safe’s relationship to PA Consulting
PA Consulting Group specialises in management consulting, technology and innovation. We have clients in both the private and public sector including higher education. We’re a firm that helps organisations harness the power of innovation and break-through technologies. 7Safe is the part of PA that provides cyber security advice, training and technical services.

How to book your place on a 7Safe course
If you know which course or courses you wish to attend, please use the Buy Now button on our website to book and pay online. Alternatively, you can book offline by calling us on 01763 285 285 or emailing us at education@7safe.com. We will then email a booking form, which is valid for seven days.

Developing a staff training programme?
7Safe is able to supply your organisation’s cyber skills training requirements, either by providing places on our public training courses or by bringing our trainers to your site to deliver a programme of courses to suit your needs.

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.

<table>
<thead>
<tr>
<th>Awareness</th>
<th>Fundamentals</th>
<th>Core</th>
<th>Specialist</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETHICAL HACKING</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Penetration Tester/Ethical Hacker</td>
<td>• CSTA Ethical Hacking</td>
<td>• CAST Advanced Web Application Security</td>
<td></td>
</tr>
<tr>
<td>• Intrusion Detection and Attack Monitoring</td>
<td>• CSTP Ethical Web Hacking</td>
<td>• CMST Mobile App Security</td>
<td></td>
</tr>
<tr>
<td>• IT Security Manager</td>
<td>• CWSA Wireless Security</td>
<td>• CSCSD Secure Coding</td>
<td></td>
</tr>
<tr>
<td>• Secure Coding for Software Developers</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DIGITAL FORENSICS
• Computer Forensics Consultant
• Cyber Security Analyst
• Data Forensics Technician
• Forensic Computer Analyst

INFORMATION SECURITY
• Hacking Awareness Training
• PCI DSS Awareness
• ISO27001 Implementation

INCIDENT RESPONSE
• Cyber Security Incident Response
• Operations Centre Analyst
• Threat Hunting

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.
ETHICAL HACKING COURSES AND CERTIFICATIONS OVERVIEW

7Safe’s 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 two 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)

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’.

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 7Safe’s 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)

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

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com
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

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.

If you are a web developer looking for a secure coding course, please see our Certified Secure Coding for Software Developers (CSCSD). See page 12.

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com

“I found it all very interesting, the hardware and software system was excellent, everything worked as planned. The content was extremely relevant to our organisation.”
CSTA Delegate
SuperWebs Ltd
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 (CTSP) 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

If you are a web developer looking for a secure coding course, please see our Certified Secure Coding for Software Developers (CSCSD). See page 12.

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com
ETHICAL HACKING  
Certified Wireless Security Analyst (CWSA)

This two-day course is for people involved in a variety of wireless network-related roles. It is designed to give you the skills you need to develop a more secure infrastructure around critical data and applications, and defend systems from unauthorised wireless attacks.

What will I learn?
- You will learn how hackers bypass wireless security, and gain an understanding of the principles of wireless cryptography
- Once able to identify and exploit vulnerabilities, you will be introduced to a range of defensive countermeasures, allowing you to complete the final exercise of building a secure wireless network to protect information assets

How will I benefit?
This course will give you:
- Valuable preparation for the CREST Registered Penetration Tester (CRT) examination
- A thorough understanding of how hackers target wireless networks and how to protect wireless networks (and clients) from attack in the real world

What qualification will I receive?
Upon successful completion of the exam, you will be awarded the Certified Wireless Security Analyst (CWSA) qualification.

Who should attend?
Anyone with responsibility for, or an interest in, the security of wireless networks and Wi-Fi enabled devices, including:
- IT managers
- Systems/network administrators
- IT security professionals
- Forensic/network investigators

CWSA prerequisites
Basic understanding of TCP/IP networking:
- Are you familiar with the OSI model?
- Can you name a layer 2 and layer 3 protocol?
- Can you describe how a request reaches a web server through Ethernet, IP and TCP?

If you are planning to do both the CSTA and CWSA courses, we recommend you take CSTA first. See page 7.

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com
ETHICAL HACKING
Certified Mobile Security Tester (CMST)

This three-day course is for people in a wide variety of mobile application-related roles. It introduces the fundamentals of mobile application security and gives you an understanding of whether the sensitive information stored on mobile devices is sufficiently protected.

**What will I learn?**
- You will be led through the current OWASP Mobile Top Ten, the most critical mobile application security risks that leave organisations and their customers’ data vulnerable to attack.
- Once able to identify and exploit vulnerabilities in both iOS and Android platforms, you will be introduced to a range of defensive countermeasures, allowing you to develop applications that are more resistant to attack.

**How will I benefit?**
This course will give you:
- An understanding of whether the sensitive information stored on mobile devices is sufficiently protected and what the risk would be if the device fell into the hands of an attacker.
- The ability to use a variety of tools and techniques, including static and run-time analysis, binary patching and reverse engineering, to improve mobile application security.

**What qualification will I receive?**
Upon successful completion of the exam, you will be awarded the Certified Mobile Security Tester (CMST) qualification.

**Who should attend?**
Anyone looking to understand the fundamentals of mobile application security, including:
- App developers
- IT security officers
- Penetration testers
- Network and systems administrators

**CMST prerequisites**
A basic understanding of:
- How the iOS and Android platform and devices work
- HTTP protocol
- Programming
- Windows and Linux command line
- Java and Objective-C languages

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com

“...I did not realise what a massive and interesting field security is. It has opened my eyes to what the hackers do to try and steal sensitive data.”

CMST Delegate
Z-Tech Control Systems Ltd
What will I learn?
- You will be led through a range of state-of-the-art hacking tools and techniques to allow you to conduct a complete web application security assessment
- Once able to identify and exploit vulnerabilities, you will learn a range of defensive counter measures, allowing you to develop applications that are more resistant to attack and provide a better protection for data assets

How will I benefit?
This course will give you:
- An industry recognised qualification, accredited by CREST and the IISP
- Essential preparation for the CREST Certified Tester (application) exam
- Security vulnerability identification and avoidance

What qualification will I receive?
Upon successful completion of the exam, you will be awarded the Certified Application Security Tester (CAST) qualification.

Who should attend?
People working in an application testing (security assessment/administration) or developer environment, including experienced:
- Penetration testers
- Application developers
- Security professionals

CAST prerequisites
- Completion of the 7Safe CSTP course or equivalent knowledge
- Practical experience of backend web application technologies (e.g. HTML, JavaScript, PHP, ASP, MSSQL, MySQL)
- Hands-on experience of modern hacking trends, tools and technologies would be an advantage

ETHICAL HACKING
Certified Application Security Tester (CAST)

This specialist four-day web hacking course is for people in a wide range of application development and testing roles. It is designed to give you an in-depth knowledge of how to identify security vulnerabilities and an understanding of the real risk that these vulnerabilities pose by exploiting them.

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com
What will I learn?
- You will learn about the vulnerabilities that arise from insecure coding and the array of hacking techniques that many attackers use to disrupt the way an application’s programming/business logic work.
- You will find out how to take a ‘defence in depth’ approach and ensure you consider all the security issues that may arise while developing applications.
- You will gain an understanding of the most important principles in secure coding and apply your new knowledge with examples and exercises in Java.

How will I benefit?
With this course, you will:
- Have access to a purposebuilt controlled environment specifically created to demonstrate the main areas of vulnerability and the key mitigation strategies.
- Get the chance to practise techniques to address common insecure coding practices.
- Build your skills and confidence in coding secure applications.

What qualification will I receive?
Upon successful completion of the exam, you will be awarded the Certified Secure Coding for Software Developers (CSCSD) qualification.

Who should attend?
This course is for people who want to learn secure coding, including:
- Penetration testers
- Professional software developers
- Software architects
- Software security auditors
- Security managers

CSCSD prerequisites
A basic understanding of web application coding, preferably in Java.

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com.

“The course was excellent and highly relevant to my work as a web developer. A variety of topics were covered and I thought that a good level of time was dedicated to the most prevalent and serious exploits.”

CSCSD Delegate
Falck Safety Services
7Safe has successfully delivered its 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.
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)

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 7Safe 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.

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com
DIGITAL FORENSICS
Certified Malware Investigator (CMI)

CORE-LEVEL COURSE

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

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

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 7Safe 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

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com

“Instructor was interesting and engaging. Obviously knew the subject well. I thoroughly enjoyed the course.”
CMI Delegate
Assured Security Control Ltd
DIGITAL FORENSICS
Certified Corporate Digital Investigator (CCDI)

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

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com
DIGITAL FORENSICS
Certified Mac Forensics Specialist (CMFS)

This specialist-level course is for experienced forensic investigators whose role requires them to expertly examine Apple devices, giving them knowledge and confidence in handling the data and forensic evidence in Mac OS X and iOS environments.

What will I learn?
- You will learn the underlying data structures of Apple devices and the many forensic artefacts specific to Mac OS X and iOS
- You will practice using real life examples identifying, finding, extracting, decoding and interpreting the data stored on an Apple device from a forensic practitioner’s perspective

How will I benefit?
This course will give you the opportunity to:
- Learn effective techniques for the identification and interpretation of forensic artefacts on OS X and iOS devices
- Understand Apple disk partitioning and develop confidence when identifying and isolating artefacts from Apple devices
- 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 Mac Forensics Specialist (CMFS) qualification.

Who should attend?
Forensic practitioners, systems administrators and cyber investigators who want to extend their experience with Window-based systems to the Mac OS X and iOS environments.

CMFS prerequisites
Completion of the 7Safe CFIP course is highly recommended. Otherwise you will need:
- Knowledge of the principles and guidelines surrounding forensic investigation
- Basic knowledge of data structures, e.g. binary and hexadecimal

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com

“An excellent course which gave a thorough overview of Mac Forensics, the HFS+ file system and important artefacts and their locations on the file system. The exercises supported the theory well and helped build on the course content. As a non-Mac user, I now feel a lot more confident working with Macs, not just for forensic analysis, but generally.”
CMFS Delegate
The Babraham Institute
DIGITAL FORENSICS
Certified Linux Forensic Practitioner (CLFP)

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

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 7Safe CFIP course is highly recommended. Alternatively you will need an understanding of digital forensic principles and practices. No Linux experience is necessary.

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com
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.

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 7Safe 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. 7Safe’s CFIP course

What 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

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com

“The course was brilliant. I really enjoyed it. It helped me to improve and develop my knowledge. I look forward to using the skills I have gained at work.”

CFIS Delegate
Computer Sciences Corporation
DIGITAL FORENSICS
Certified Cyber Investigator (CCI)

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 7Safe CFIP and CLFP courses as a minimum before attending this course.

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com

“This was the most useful networking investigation course I have been on in recent years. I came away with a substantial increase in my knowledge along with some very useful documentation. If you’re going to do one networking investigation course a year, make it this one.”

CCI Delegate
Regional Cyber Crime Unit
INFORMATION SECURITY TRAINING COURSES AND CERTIFICATIONS OVERVIEW

7Safe’s 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. The courses last between one and three days and provide a high-level understanding of the techniques and current trends used in hacking or the steps involved in planning, implementing and maintaining ISO 27001 or Payment Card Industry Data Security Standard (PCI DSS).
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 nontechnical staff and no prior knowledge is required.

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com
INFORMATION SECURITY
Payment Card Industry Data Security Standard (PCI DSS) Implementation

What will I learn?
• You will gain a clear understanding of the PCI DSS and how to apply your knowledge when assisting with PCI DSS assessments
• You will learn how the Standard developed, its benefits and who it applies to
• You will find out about the key requirements of the Standard and how to become compliant

How will I benefit?
With this course, you will:
• Gain an appreciation of the controls necessary for your organisation to be able to continue dealing with cardholder data
• Learn the key principles and requirements of the Standard
• Develop an understanding of the route to compliance (self-assessment and audit)
• Be in a position to prepare an implementation plan for your organisation, improving your chances of a successful audit

Who should attend?
This course is for:
• Anybody accepting credit card payments, including:
  • Merchants
  • Third-party service providers
  • Acquirers
• Anybody processing, storing or transmitting credit card data
• Finance, internal audit, IT, sales department staff

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

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com
INCIDENT RESPONSE & SOC TRAINING

These 7Safe-designed 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.

7Safe’s 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 organisation’s 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

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 organisation’s incident response plan

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com
INCIDENT RESPONSE
Certified Security Operations Centre Analyst (CSOCA)

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 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.

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com
INCIDENT RESPONSE
Cyber Security Incident Response (CSIR)

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 7Safe CFIP and CMI courses or similar as a minimum before attending this course.

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com
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.

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com
MSc in Professional Practice in Digital Forensics and Security

This programme, delivered in partnership with De Montfort University (DMU), is for people who want to gain a postgraduate-level qualification in information security. This qualification is based on 7Safe’s technical hands-on training courses, combined with academic modules delivered by the University.

What will I learn?
- You will acquire a thorough and practical knowledge of the very latest computer forensics and security principles, practices, tools and techniques. The key modules covered are: network security and ethical hacking, wireless security, forensic investigations, malware investigations and implementing ISO 27001
- You will gain an understanding of the main academic, professional and research concerns of computer security and forensics through a research-led module that will help prepare you for your MSc project/dissertation

How will I benefit?
This course will provide you with:
- The latest tools, techniques and knowledge in one of the most exciting areas of modern computing
- Expert staff with extensive experience in the field of forensics and security
- Excellent career prospects in a rapidly expanding industry

What qualification will I receive?
The MSc course consists of seven 7Safe training courses (CSTA, CSTP, CWSA, CFIP, CMI, CFIS and CIIP), eight University modules and an MSc project/dissertation. Upon successful completion of the MSc, you will therefore have seven industry-recognised professional certificates as well as the MSc qualification.

Who is this course for?
Anyone ambitious to build a career in information security by completing a part-time or full-time post-graduate course. When taking the course as a part-time pathway you should expect to study for a minimum of two to three years, and must be completed within six years.

MSc prerequisites
After successfully completing one or more 7Safe courses, the MSC is the most practical and natural progression to further your cyber knowledge and career development.

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email education@7safe.com
www.7safe.com