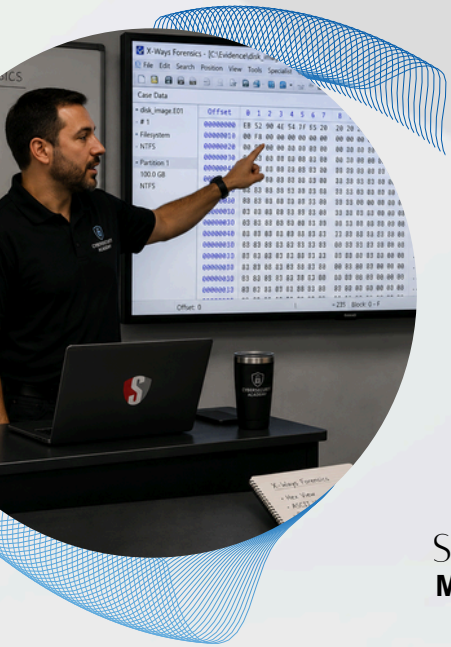
SIKER

Cyber Security Training Prospectus

BELIEVE
LEARN
ACHIEVE

CONTENTS



“Our training programmes are of the highest quality, and we look forward to working with you to combat the cyber threat.”

STEVE SHEPHERD MBE
Managing Director & Head of Academy

CYBER SECURITY TRAINING AT SIKER

Cyber Security & Digital Forensic Investigations are rapidly growing areas within the industry today, and skills in this area are in high demand.

SIKER CYBER SECURITY TRAINING

Our courses are designed and delivered by industry professionals and academics. Our aim is to deliver training in the disciplines of data recovery, digital forensics, malware investigations, cybersecurity incident response, and mobile phone investigations.

SIKER PASSPORTS

Training passports offer discounted rates across all our cyber disciplines, including OT. Simply purchase a set number of training days at the discounted rate (e.g. 160 or 240 hours) and save on the cost of booking courses individually.

TRAINING DELIVERY METHOD

Siker offers three delivery methods:

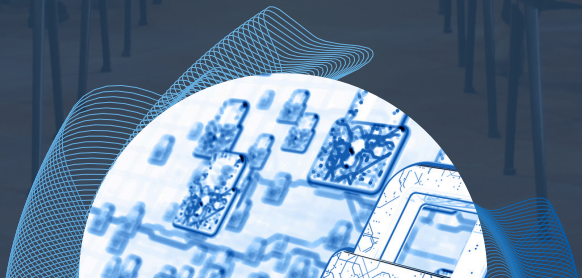
- Virtual on demand
- Virtual face-to-face
- Classroom-based (various venues)

ON-SITE TRAINING

For groups of 8 or more, we can deliver exclusive on-site (or remote) training from our existing suite of courses.

BESPOKE TRAINING

We can create bespoke training for organisations that require specific content.



ABOUT SIKER

Siker's roots began with the development of cyber training programmes for industry. Siker specialises in OT cyber security training and business development for industrial organisations, as well as in developing cyber security capability and training programmes for clients in the UK and abroad.

HOW TO BOOK YOUR PLACE ON A SIKER COURSE

Know which course you want to attend? Please press the Buy Now button on our website https://sikercyber.com or contact us online by emailing education@sikercyber.com. You will receive a booking form via email, which will be valid for 7 days.

OUR CYBER TRAINING PORTFOLIO AT A GLANCE

	Awareness	Fundamentals	Intermediate	Advanced
Ethical Hacking	HIM			
Digital Forensics	DFIM	DFI LDF FDC	DFA LDFA FDCT	ADFP
Malware Investigations	MFIM	MFI	MFA	AMFP
Cyber Security Incident Response	CSIRM			CSIR 1

ETHICAL HACKING TRAINING OVERVIEW

Our training programme aims to help organisation leaders and managers to understand the threats to business systems.

ETHICAL HACKING TRAINING

HACKING INSIGHT FOR MANAGERS (HIM)

This one-day awareness course is designed for people who need a high level of understanding of hacking, rather than the level of knowledge and ability expected of a cybersecurity practitioner.
The course introduces the fundamental technical concepts underlying the stages of a hacking attack, as well as some standard tools used by both hackers and security professionals. Delegates will receive a certificate of attendance.

DIGITAL FORENSIC TRAINING & CERTIFICATIONS OVERVIEW

Our training programme aims to help cyber and digital forensics investigators and practitioners enhance their skills through practical, hands-on experience. Our experienced trainers will provide the most up-to-date industry best practices and tools for successful cyber and digital forensics investigations.

DIGITAL FORENSIC TRAINING

DIGITAL FORENSIC INVESTIGATIONS FOR MANAGERS (DFIM)

This one-day awareness course is designed for people who need a high level of understanding of hacking, rather than the level of knowledge and ability expected of a cybersecurity practitioner. The course introduces the fundamental technical concepts underlying the stages of a hacking attack, as well as some standard tools used by both hackers and security professionals. Delegates will receive a certificate of attendance.

INTRODUCTION TO DIGITAL FORENSIC INVESTIGATIONS (DFI)

This three-day foundation course is tailored for individuals new to, or recently entering, the digital forensics field. It aims to provide a solid foundation in digital forensic principles, with a focus on data structures and artefacts produced by the Windows operating system. The course also offers an overview of the NT file system's data structures. Delegates will receive a certificate of attendance.

DIGITAL FORENSIC ANALYST (DFA)

A five-day intermediate course designed for those involved in digital forensics or related disciplines to strengthen their skills in identifying and analysing data structures generated by the Windows operating system. The course also covers the data structures of the FAT and NT file systems. This certified course requires delegates to pass the accompanying theory and practical exams to obtain certification.

ADVANCED DIGITAL FORENSIC PRACTITIONER (ADFP)

This five-day course is designed for individuals with experience in traditional digital forensics or related fields who wish to enhance their skills in investigating a live network environment (Windows Domain). Participants will learn to identify network devices and user account information and to investigate remote nodes. The course also reviews the data structures of the FAT, NT, and exFAT file systems. This is a certified course, and delegates must pass the accompanying theory and practical exam to obtain certification.

DIGITAL FORENSIC TRAINING CONT.

INTRODUCTION TO LINUX DIGITAL FORENSICS (LDF)

This is a three-day foundation course for digital forensic practitioners seeking to enhance their knowledge and practical skills for investigating Linux-based computers. Delegates will be introduced to the ext3 and ext4 file systems used by Linux-based systems. Delegates will receive a certificate of attendance.

LINUX DIGITAL FORENSIC ANALYST (LDFA)

This is a five-day intermediate course for digital forensic practitioners with some experience who wish to improve their knowledge and practical skills in navigating, identifying, capturing and examining data from static and live Linux-based systems. The course also covers the examination and analysis of ext3 and ext4 file systems. This is a certified course, and delegates must pass the accompanying theory and practical exam to obtain certification.

INTRODUCTION TO FORENSIC DATA COLLECTION (FDC)

This three-day foundation course is designed to build confidence and provide a basic understanding for individuals interested in, or new to, the role of collecting data from computers and media. The course will equip delegates with the knowledge and skills to identify and preserve data, ensuring it can be safely copied from its source to a storage medium while maintaining its integrity. Delegates will receive a certificate of attendance upon completion of the course.

FORENSIC DATA COLLECTION TECHNICIAN (FDCT)

This five-day intermediate course is for individuals responsible for collecting data or advising on data collection. It will equip participants with the skills needed to ensure the integrity of data gathered or copied from various sources, including static and volatile environments, and to withstand scrutiny in legal proceedings. This is a certified course, and delegates must pass the accompanying theory and practical exam to obtain certification.

MALWARE TRAINING & CERTIFICATIONS OVERVIEW

Our malware training programme aims to help cyber and digital forensics investigators understand how malware can infect a computer, how it can evade detection, and the methods that can be used to identify malware capabilities.

MALWARE INVESTIGATION TRAINING COURSES

MALWARE FORENSIC INVESTIGATIONS FOR MANAGERS (MFIM)

This one-day awareness course is designed for personnel who may need to understand or manage cyber investigations involving malware. The course covers different malware types, their capabilities, and how some complex malware can evade detection. Delegates will receive an attendance certificate.

INTRODUCTION TO MALWARE FORENSIC INVESTIGATIONS (MFI)

This three-day foundation course combines theory with practical exercises, focusing on the principles of malware investigation. It covers fundamental knowledge of malware types, their capabilities, and the investigation techniques used to detect the presence, infection, and persistence of malicious software. Delegates will receive a certificate of attendance.

MALWARE FORENSIC ANALYST (MFA)

This is a five-day intermediate practical course designed for individuals seeking to expand their knowledge and skills in forensic malware investigation. It covers malware types, capabilities, and common techniques to consider when conducting live investigations of malicious software to identify presence, infection, and persistence. The course will conclude with a practical exercise focused on malware analysis and investigation methodology. This is a certified course, and delegates must pass the accompanying theory and practical exams to obtain certification.

ADVANCED MALWARE FORENSIC PRACTITIONER (AMFP)

This five-day, advanced technical course is a specialist-level programme for individuals seeking to extend their knowledge beyond traditional malware investigations. Building on our intermediate Malware Forensic Analyst (MFA) course, it provides delegates with a deeper technical understanding of how to investigate suspected complex malware infections. You will apply the knowledge, methods, and techniques learned during the course to identify and remediate complex malware that traditional antivirus and security solutions might not detect. The course concludes with a practical exercise to reinforce key learning points. This is a certified course, and delegates must pass the accompanying theory and practical exams to obtain certification.

CYBER SECURITY INCIDENT RESPONSE TRAINING & CERTIFICATIONS OVERVIEW

These Siker-designed training courses are for leaders, managers and professionals seeking to develop or improve their knowledge and ability in the discipline of Cyber Security Incident Response (CSIR).

CYBER SECURITY INCIDENT RESPONSE TRAINING

CYBER SECURITY INCIDENT RESPONSE FOR MANAGERS (CSIRM)

This one-day awareness course is designed for personnel who may need to manage a response to a cyberattack or breach. It covers incident response preparation and the fundamentals of incident management. Delegates will receive an attendance certificate.

CYBER SECURITY INCIDENT RESPONDER (CSIR 1)

This five-day advanced course is designed for CSIR professionals or individuals seeking to develop their skills and knowledge to enter this field. The programme covers the essential knowledge required of an incident response practitioner, along with practical exercises to enhance skills and retention. Delegates are also expected to undertake self-study during the course due to the volume of content. This is a certified course, and participants must pass the accompanying practical and theory exams to obtain certification.

CYBER TRAINING IN DEVELOPMENT

We keep our cyber courses regularly up to date with the latest tools and techniques where relevant. We also review industry requirements and create new courses based on industry needs.

COURSES IN DEVELOPMENT

INTRODUCTION TO MOBILE PHONE FORENSICS (MPF)

This is a three-day foundation course covering the investigation of Android-based mobile devices. It will provide an overview of the most popular messaging and social media applications, including Telegram, WhatsApp and Snapchat. Delegates will receive a certificate of attendance.

MOBILE PHONE FORENSIC ANALYST (MPFA)

This is a five-day intermediate course on the investigation of Android-based mobile devices. The course will cover the analysis of applications and databases, as well as the manual decoding and analysis of popular applications, including the creation of an emulated Android device for analysis that delegates can take home. This is a certified course, and participants must pass the accompanying practical and theory exams to obtain certification.

MOBILE PHONE MALWARE ANALYST (MPMA)

This is a five-day intermediate course on investigating malware-infected Android-based mobile devices. The course will cover static and dynamic analysis of Android malware, including reverse engineering of the malware code. This is a certified course, and participants must pass the accompanying practical and theory exams to obtain certification.

CYBER SECURITY INCIDENT RESPONDER 2 (CSIR 2)

This is a five-day advanced course in Cyber Security Incident Response, focusing on PowerShell and creating scripts to automate data collection from myriad locations, including automated RAM dumps from Windows-based machines.

“I look forward to working with you to combat the cyber threat. I can affirm that our Siker cyber training programmes are of the highest quality.”

Tim Harwood
Chief Executive Officer

education@sikercyber.com

+44 (0)20 3441 7642

https://sikercyber.com

@sikercyber

https://www.linkedin.com/company/siker-cyber

https://www.facebook.com/SikerCyber

CFL Cyber