



OT CYBER
SUMMIT 2023

ABU DHABI

28th August –
8th September

Fairmont
Bab Al Bahr
United Arab
Emirates

Use code 'earlybird10' for 10% discount



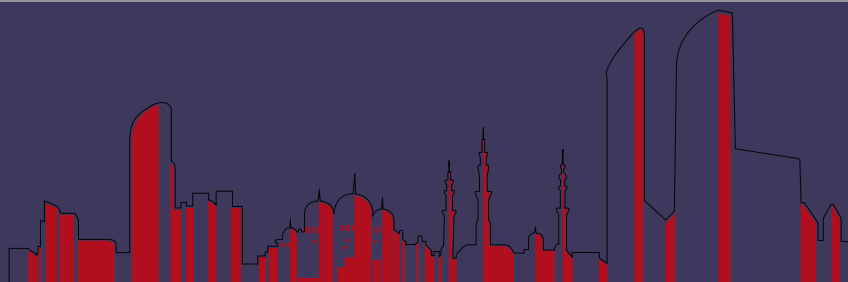
THE OT CYBER TRAINING SUMMIT

The new OT cyber event of the 2023 calendar. Come along and join us for two weeks of Internet Cyber Security courses and accreditations, enabling you to take away valuable skills and knowledge to use and develop in your role.

We have courses to suit all levels of skill and experience, with optional exams included. From one day to five days, you can build your schedule of learning to suit you.

We have world renowned trainers leading each course. During the summit you'll have the opportunity to network, drawing on over 100 years of industry experience between them! The event also provides a great opportunity to engage with other industry experts from around the globe.

All set in the beautiful surroundings of Fairmont Bab Al Bahr, Abu Dhabi.



ABOUT SIKER

A cyber security training, evaluation and investigation specialist operating globally since 2013 to meet the needs of clients.

When Siker first launched its whole ethos was about providing people with the right level of skills to be able to perform their job and their role securely. We recognised that not everyone needs to be a security professional but most of the users of today's IT do need to understand more about how they can become 'professionally secure'.

We help organisations fully understand how their staff can become part of their first line of defence and thus, reduce their attack surface and the organisation's risk profile.

Platinum

We are delighted to be joined by our partner Platinum 3P. Platinum 3P provide subject matter expertise to support clients in their endeavours to counter terrorism and crime. They provide consultancy services, including the full consulting cycle support, active interventions and advice, as well as training in the area of terrorism and crime prevention.



Securing ICS

Level: 4 - Senior Practitioner

**Commences:
4th September**

**Duration:
5 Days**

**Cost:
\$4750 USD**

This course is to provide those at IT/operational level (or equivalent) with an understanding of today's cyber security challenges facing their ICS environments. Show how to combine the disciplines of IT, Operational Technology (OT), physical security and facilities management and how to best support your organisations cyber security and risk mitigation strategies.

You will learn:

- What exactly is an ICS?
- Identify what current and emerging threats your ICS environments face.
- Where your ICS environments may be vulnerable.
- What actions you need to take to secure those environments and help reduce the risk.
- Prepare for and manage a cyber security incident in those environments.
- Prepare for challenging the GICSP exam.



Instructor:

Tim Canning

ICS Practitioners Security

Level: 2 - Foundation

Commences:
28th August

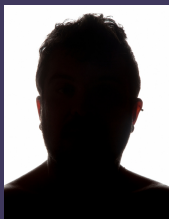
Duration:
2 Days

Cost:
\$1920 USD

An APMG accredited course which will provide practitioners with an understanding of today's cyber security challenges facing their ICS environments. This knowledge is vital when managing the day to day running of all aspects of security risk for those environments. Show how to best protect and support your organisations cyber security and risk mitigation/reduction strategies.

You will learn:

- Identify the current and emerging threats to your ICS environments.
- Where your ICS environments may be vulnerable.
- What actions you may need to take to secure those environments and help reduce the risk. to your organisation, nation and supply chain.
- Prepare for and handle a cyber security incident in an ICS environment.
- The need for structured Security Awareness and Training.



Instructor:

TBC

Open Source Internet Investigation (OSINT)

Level: 2 - Foundation

Commences:
30th August

Duration:
3 Days

Cost:
\$2820 USD

Hands on, practical and immersive module suitable for those who use the internet to conduct overt open source investigations or intelligence research. Ideal for those who have little or no knowledge of OSINT.

You will **learn**:

- Apply basic and advanced internet search techniques.
- Apply appropriate evidence capture methodologies in internet investigations.
- Identify evidential and intelligence opportunities to develop internet investigations.
- Apply appropriate safeguards when operating online to protect tactics including anonymisation.
- Demonstrate the investigative value of digital images, domains and websites.
- Demonstrate the tracing of subjects and commodities through current and historic websites, and IP addresses using specialist network investigation techniques.
- Demonstrate basic levels of investigation of social media content.
- State legislation and procedural practices which may influence internet investigations.



Instructor:

Gavin Mee

Cyber Investigator – Foundation

Level: 2 - Foundation

Commences:
4th September

Duration:
3 Days

Cost:
\$2820 USD

This is a hands on, practical and immersive module suitable for those who investigate Cyber Enabled and Cyber Dependent Crime. You will learn to do the following:

You will learn:

- Identify cyber dependent and cyber enabled crime.
- Types and functions of malware.
- Role of the cybercrime first responder.
- Prepare a cybercrime investigative strategy or plan.
- Concepts of computer networks and how they relate to a cybercrime investigation.
- Concepts of digital forensics in a cybercrime investigation.
- Identify, secure and preserve digital evidence.
- Value and use of open source information in a cybercrime investigation.
- Role of authorisations, procedures and policies in a cybercrime investigation.
- Prepare a risk management plan in relation to a cybercrime investigation.
- Prepare and present cybercrime material to a prosecutor.



Instructor:
Jon Blake

ICS Industrial Control Fundamentals for All

Level: 1 - Awareness

Commences:
28th August

Duration:
2 Days

Cost:
\$1920 USD

Provide an introduction into aspects of Operational Technology design and use in industrial applications, and provide an understanding of ICS design, configuration, operations and maintenance principles in a real-world context. Students will create a simple ICS design to aid understanding and retention.

You will learn:

- Process sensor basics.
- How sensors communicate to controllers.
- How controllers make decisions.
- How controllers manage machinery.
- The basics of industrial communications.
- Human Machine Interface fundamentals.
- Foundation concepts of operational and machinery safety.



Instructor:

Tim Canning

ICS Security Incident Response Fundamentals

Level: 2 - Foundation

Commences:
30th August

Duration:
2 Days

Cost:
\$1920 USD

Gain an understanding of the security risks to today's ICS environments. What can be done to prepare for, respond to, and subsequently recover from a cyber incident that affects the control system or part of it.

You will learn:

- How to articulate the difference between an Incident and an Event and be able to identify both.
- How to use the 6-stage process for Incident Response.
- How to Identify the key roles that make up a standard Incident Response Team.
- The legal and regulatory aspects of cyber incident response.
- How to handle different types of incidents.



Instructor:

Tim Harwood

ICS Managers Security Fundamentals

Level: 1 - Awareness

Commences:
1st September

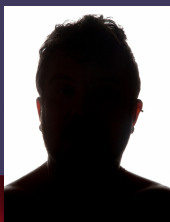
Duration:
1 Day

Cost:
\$995 USD

This course will show students how to best identify and support their organisation's cyber security and risk mitigation/reduction strategies for their ICS environments.

You will learn:

- ICS Cyber risk including the constraints and associated drivers within the Cyber-Physical environments.
- What help is available to aid you in creating effective and usable cyber programs.
- The likely areas of weakness in your ICS environment.
- Where your ICS critical assets may be vulnerable.
- What the organisational response to an ICS security incident should look like (and your responsibilities in effectively managing these).
- The need for ICS security awareness and training.



Instructor:

TBC

ICS4ICS Workshop

Level: 1 - Awareness

**Commences:
7th September**

**Duration:
1 Day**

**Cost:
\$100 USD**

This workshop will cover the basics of the ICS4ICS program. Incident Command System for Industrial Control Systems (ICS4ICS) is designed to improve global Industrial Control System cybersecurity incident management capabilities. ICS4ICS will leverage the Incident Command System, as outlined by FEMA, for response structure, roles, and interoperability.

Sessions include:

- Welcome and Introduction to ICS4ICS.
- Cyber security basics.
- Industrial Control Systems.
- Incident Command System used to manage incidents
- Use the Planning 'P'.



Instructor:

Tim Harwood

Meet the Instructors



TIM HARWOOD
SIKER CEO

Tim Harwood is a veteran of the security world and has been providing information security guidance and expertise to corporate clients, the UK Government and the UK military for over 30 years. As CEO of Siker, he provides strategic direction for the company that he founded in 2013. Tim's professional background includes security capability strategy planning and development, information security capability framework design and security awareness strategy design. He has developed a security professional development framework for a global top ten oil and gas company, delivers training as a member of the QA and Firebrand faculties.

Tim has designed and delivered ICS security training and awareness for CPNI/NCSC (as part of the UK National Cyber Security Strategy) as well as ENISA and other National governments and global companies. He is also a Visiting Lecturer on Business Risk at the University of Buckingham.



JON BLAKE

**PLATINUM 3P CEO AND
SIKER ADVISORY BOARD**

Jon has over 28 years' detective experience as an investigator and covert intelligence specialist with the Metropolitan Police Service, New Scotland Yard, London. He specialises in Internet and cybercrime investigation, covert operations and related risk. He retired from the service in 2014 with an exemplary service record.

Jon contributes to a number of working groups as a subject matter expert in the areas of Internet related crime and covert operations and acted as an advisor to those setting national investigative policy and procedures.

Jon is a sought-after speaker, trainer, and university lecturer, and regularly undertakes speaking engagements in the UK and overseas. He holds several cyber industry certifications



TIM CANNING
SENIOR ICS
CONSULTANT AND
TRAINER

Tim is an experienced Ops Technology Cyber-Security Engineer having upskilled over a decade ago following a long career working in Process Automation, Controls and Instrumentation for System Integrators, Tier-1 and -2 Engineering Contractors, and International Oil and Gas Operator companies. Tim is a current holder of the GICSP certification, as well as the Certified Ethical Hacker (CEH) and various professional technical certifications. He has delivery experience in Operational Technology Cyber-Security improvements to live plant and systems complemented by experience as a certified Functional Safety Engineer.

An experienced Intelligence, Security and Risk Management professional who was formerly a member of the British Army Intelligence Corps. Gavin has a strong background in the effective utilisation of OSINT for a range of clients and projects including due diligence and background checking, investigations, online vulnerability and threat assessments and asset tracing. Additionally, Gavin has led and advised on the establishment of OSINT teams, infrastructure and software for a range of organisations, and subsequently mentored their staff.



GAVIN MEE
PLATNUM 3P SENIOR
ASSOCIATE TRAINER

Join us

For more information visit
sikercyber.com

Email enquires to
summit@sikercyber.com

Use the code *earlybird10* to get
10% off.*



*Offer ends 25th June 2023