cSEMINAR INFORMATION SECURITY SPECIALISTS

No organisation today can do without modern information and communication technology (ICT). However, this technology is driven by performance and services, rather than security. As a consequence, the really important asset – i.e. the information – is subject to different risks. This is especially relevant in the highly sensitive areas of government and defence, where comprehensive security must be ensured by highly qualified security specialists. The unequaled growth rate of technological crime makes the stakes even higher.

Crypto AG offers a compact 5-day professional seminar in security fundamentals for decision-makers and security or system managers. The seminar will help participants expand their expertise in ICT security fundamentals. The focus of the Crypto cSeminar will be on how to effectively counter man-made risks, and identify the requirements to be met by solutions.

The contents of the cSeminar Information Security Specialists are managed by the highly experienced and specialised training engineers at the Crypto Academy. Theory and practice are carefully balanced; discussion of examples and case studies, and practical sessions, are given preference over academic presentation. The curriculum of the seminar is in continual evolution; therefore, the contents are regularly checked and updated. New materials or new issues are included according to the evolution of the risk scenario.

This seminar will be held at our very own Crypto Academy in Steinhausen / Zug, Switzerland, which has been awarded a "Premium Class" rating from the International Training Centre Rating Organisation. The comfortable and pleasant atmosphere and the highly qualified instructors will ensure that you will have a successful learning experience.

Course objectives

Participants will be provided with a working model of information security which they can apply to their own organisation. Information which is often available from different sources is made available in a consistent tutorial structure which alternates theory, practice and discussion. Delegates receive in-depth information on the latest developments in threats, technological crime, and defence methods.

Who should attend

This seminar is open to all participants who typically belong to staff of the IT, communications, signals, or other technology-related departments. Their responsibilites include planning, operating, maintaining, improving, evaluating and auditing risk management and information security management processes. Delegates should have a good working knowledge of IT and communications fundamentals and understand concepts such as networking, cloud computing, and IT services.

Certification

All participants receive a Certificate of Attendance to the five-day training event.

Standard seminar package

The standard seminar package includes transport, accommodation, catering and leisure activities during the entire stay organised by Crypto AG. Don't hesitate to contact us if you have any change requests or further questions.

For registration and upcoming seminar dates please visit the website www.crypto.ch/seminars

The standard seminar package costs 7,100 CHF.

CONTENT

Agenda

Day 1 — Political espionage, cyber crime and information warfare

The seminar starts with an introduction of the most common threats and risks accompanied by several live demonstrations on how to steal or forge different information assets.

- Introduction and overview
- Definitions, threats and dangers
- Common actors and enemies
- Current state of things
- Timeline of a hacker attack
- Investigation and research
- Scanning and sniffing
- Taking control, shutting down
- Setting up backdoors
- Covering the traces
- Example of risk areas
- Defence in-depth

Day 2 — Security Awareness

Information Security, in most cases, is only looked at from technical and organisational perspectives. Practice, however, shows that the main threat is still posed by unwitting actions of personnel. This module will show the most common areas of risk and provide an indication on how to address this specific risk.

- The risks of the human factor
- Attacks against people
- Building awareness
- Basic threats and security services

Day 3 — Cryptography

Cryptographic measures support the security of information, whether being processed, stored or transmitted. This module will teach participants the basics of cryptography, with its different schemes, their pros and cons: symmetric and asymmetric algorithms, including appropriate key management.

- Symmetric crypto systems
- Asymmetric crypto systems
- Services and mechanisms
- Key establishment mechanisms
- Key management

Day 4 — Evaluation of crypto systems

Verifying the correct implementation and assessing the strength and effectiveness of security functions is a vital part of the selection process. This module informs participants of the relevant standards and procedures.

- Requirements for evaluation
- Standards and their history
- Common criteria and ISO 15408
- CC and CEM
- Evaluation documentation
- Evaluation process

Day 5 — Introduction to best defence security practice

Closing the seminar, this module introduces the information security management process, based on the acknowledged ISO 27001 international standard.

- Introduction to the security process
- Introduction to the ISMS standards
- Risk management
- Implementation of an ISMS
- Introduction to business continuity
- Conclusion

Information and specifications are subject to change without notice.

Restricted © Crypto AG. All rights reserved. cSeminar for Information Security Specidlists / EN / 1611