

KAÏNA-COM TRAINING CATALOGUE

Mobile Devices Security



Nos locaux
KAÏNA-COM France
LE CARRÉ HAUSSMANN II
6 Allée de la Connaissance
77 127 Lieusaint



Contact
+33(0)9 50 20 91 64



E-mail
info@kaina-com.fr



Site Internet
www.kaina-com.fr

KSE007 – Mobile Devices Security

Reference KSE007

Experience

- Beginner
- Intermediate
- Advanced

Duration Training Program:

- 2 days

Training Method

- I: i-learning, individual training (web-based training)
- V: v-learning, virtual class
- C: c-learning, classroom training

KAÏNA-COM
LE CARRÉ HAUSSMANN II,
6 Allée de la Connaissance
77127 Lieusaint - France

Price 1.390,50 € HT

Prerequisite Knowledge of IP, SIP and basic networking.

Audience This course is recommended for IT managers

Continued on next page



KSE007 – Mobile Devices Security, Continued

Objective

The Smartphone today is vulnerable and open to many potential attacks. In many cases organizations implement the BYOD while employees may download various applications that some of them may include malicious software, malware, and viruses. These threats may cause tremendous damage to companies.

Continued on next page



Nos locaux
KAÏNA-COM France
LE CARRÉ HAUSSMANN II
6 Allée de la Connaissance
77 127 Lieusaint



Contact
+33(0)9 50 20 91 64



E-mail
info@kaina-com.fr



Site Internet
www.kaina-com.fr

KSE007 – Mobile Devices Security, Continued

Course Contents

Course Contents :

Table 1: KSE007 - Course Contents

Chapter	Description
Security Threats	<ul style="list-style-type: none"> • Security Criterias • External and Internal threats • Classic Threat Models
Security building blocks	<ul style="list-style-type: none"> • FW, NAC and SBC • IDS and IPS • MDM versus Container
Mobile Device Management (MDM)	<ul style="list-style-type: none"> • The concept of MDM • Mobile Information Management (MIM) • Geolocation concept • Mobile Application Behavioral Analysis
Encryption methods for mobile clients	<ul style="list-style-type: none"> • Public and Private keys • Symmetric and Asymmetric encryption keys • DES and Triple DES
Encryption protocols for mobile clients	<ul style="list-style-type: none"> • TLS • VPN and IPsec • Media encryption- SRTP • S/MIME
Secured Telephony Clients for Mobile devices	<ul style="list-style-type: none"> • SIP Client • Protection against MIM: Encryption

Continued on next page



KSE007 – Mobile Devices Security, Continued

Course Contents, continued

Chapter	Description
Authentication by secured client	<ul style="list-style-type: none">• HTTP digest authentication• Lightweight scheme for authentication• Authentication Challenges
Containers for mobile devices	<ul style="list-style-type: none">• The challenges• Container concept• Protection methods• Mails and Messages encryption
Session Border Controller (SBC)	<ul style="list-style-type: none">• NAT Traversal and FW penetration• Encryption functionality – TLS, SRTP, SDES, ZRTP, DTLS• Lawful interception• DoS and DDoS immunity• Deep Packet Inspection (DPI at all layers)
The End	<ul style="list-style-type: none">• MLP- Multi-Layered-Protection concept• Vendors for Mobile protection• Penetration Tests• Q&A• Course's Evaluation

