Catalogue de Formation
15/06/2020

KAÏNA-COM
CATALOGUE DE FORMATION

Fondements de la cybersécurité et IA

Étudier les fondements de la cybersécurité et donner un aperçu de l'environnement de sécurité moderne et une introduction à l'IA

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

KBP003 – Fondements de la cybersécurité et IA

Référence	KBP003
Niveau	☒ Débutant ☒ Intermédiaire ☐ Expert
Nombre de Jours	40 h (10 jours)
Lieu de la formation	☐ I: e-learning, Formation individuelle (Formation en ligne) ☒ V: v-learning, classe virtuelle ☐ C: c-learning, cours présentiel **KAÏNA-COM** LE CARRÉ HAUSSMANN II, 6 Allée de la Connaissance 77127 Lieusaint - France
Prérequis	Connaissance de base des réseaux IP. Un niveau d'anglais business moyen est requis car la formation sera dispensée en anglais.
Public	Cadre de haut niveau, ingénieur avant-vente, responsable informatique, QA et support technique, programmeur et étudiant désireux d'en apprendre davantage sur la cybersécurité et l'IA.

Ce sujet continue à la page suivante

KBP003 – Fondements de la cybersécurité et IA, Suite

Objectifs

L'objectif principal du cours de cybersécurité est de couvrir les sujets fondamentaux de la cybersécurité, de fournir un aperçu de l'environnement de sécurité moderne, le paysage de la cybermenace et la mentalité des attaquants, y compris la façon dont les attaquants travaillent, quels outils utilisent-ils ? quelles vulnérabilités ciblent-ils?

Avec des tutoriels interactifs qui permettent à chaque participant d'apprendre à son rythme avec un suivi personnalisée.
Chaque sujet est abordé sur le plan à la fois théorique et pratique, afin que les participants puissent obtenir de l'expérience, ce qui rendra l'étude plus efficace.

Ce sujet continue à la page suivante

KBP003 – Fondements de la cybersécurité et IA, Suite

Contenu du cours

Contenu du cours :

Table 1: KBP003 - Contenu du cours - Cyber Security (Meeting#1)

Chapitre	Contenu
Introduction to Cyber Security	• Hacking History • Cyber Attacks Trends • External and Internal threats • Hackers Types • Threats and attacks • Security Criteria's • Threat Taxonomy Models summary
Basics of Security Management	• Security Layers • Defending concept according OSI Layers • Security modules and functionalities • NAT- Network Address Translation • Firewalls Types • Network Access Control (NAC) • IDS and IPS • Encryption protocols: IPSec, TLS and SRTP • Replay Attacks Protection • Server Hardening

Ce sujet continue à la page suivante

KBP003 – Fondements de la cybersécurité et IA, Suite

Contenu du cours, Suite

Table 2: KBP003 - Contenu du cours - Cyber Security (Meeting#2)

Chapitre	Contenu
TCP/IP vulnerabilities	• Network Layer (IP) services – 3rd Layer • IP Header Structure • MTU and Fragmentation process • IP Addressing – issues and solutions – ARP, DHCP, NAT • Transportation Layers: TCP, UDP, SCTP
Introduction to Cryptography	• Public and Private keys • Symmetric and Asymmetric encryption keys • DES and Triple DES • AES and RSA methods

Table 3: KBP003 - Contenu du cours - Cyber Security (Meeting#3)

Chapitre	Contenu
MiTM challenge and confidentiality solutions	• What is TLS • What is IPsec • Applications over TLS and IPsec
Inspection and interception Tool – Hands-on	• Introduction to Wireshark • Getting Started • Capturing Packets • Color Coding • Sessions Filtering methods • Inspecting Packets • Network Topology studying • MAC Addresses and manufacturers • 3rd layer and IP Addresses analysis • Open ports at 4th Layer Analysis • Call flow analysis • Traffic analysis and eavesdropping • Live capture and real-time interception

Ce sujet continue à la page suivante

KBP003 – Fondements de la cybersécurité et IA, Suite

Contenu du cours, Suite

Table 4: KBP003 - Contenu du cours - Cyber Security (Meeting#4)

Chapitre	Contenu
Firewall	• PFF, Proxy GW, Stateful Inspection • Management menu • Rules and policy
IPTables Firewall	• What is IPTables? • Chains and Chain Policy • Creating Rules and Rules Examples • Connection States • User Defined Chains • Logging Events/Packets • Advanced Examples • Managing IPTables Firewall
Network and Vulnerabilities Scanning	• Basic Scanning Techniques • Discovery Option • Operation System Detection • Nmap Script Engine • Nmap GUI • Vulnerabilities Information Sources • Vulnerabilities Scanners

Ce sujet continue à la page suivante

KBP003 – Fondements de la cybersécurité et IA, Suite

Contenu du cours, Suite

Table 5: KBP003 - Contenu du cours - Cyber Security (Meeting#5)

Chapitre	Contenu
Kali Linux	• What is Kali Linux? • Some Kali Facts • Installing Kali Linux • Tools Categories • Kali Desktop • Kali Top Tools • Kali Linux Alternatives
Network Scanning – Demo	• NMAP - Networks Scanning for Topology analysis and network Mapping • OpenVAS for vulnerabilities scanning and analysis

Table 6: KBP003 - Contenu du cours - Cyber Security (Meeting#6)

Chapitre	Contenu
Services inspection – Demo	• Numbers Harvesting • Conferences eavesdropping • Password capture
Firewall – Demo	• FW Rules setting • Denial of Service and DDoS attacks • Port scanning and vulnerabilities • Blocking scenarios
Certificates and Authenticati on process	• Certificates and X.509 ITU-T Standard • HTTP digest authentication • Authentication scheme for a trusted domain • Authentication Challenges

Ce sujet continue à la page suivante

KBP003 – Fondements de la cybersécurité et IA, Suite

Contenu du cours, Suite

Table 7: KBP003 - Contenu du cours - Cyber Security (Meeting#7)

Chapitre	Contenu
Penetration Testing	• What is Penetration Testing? • Reasons for Pen Testing • Hackers and Pen Testing • Vulnerabilities • What do we test? • Pen Testing Phases • Types of Testing • Areas of Penetration Tests • References
Network Penetration – Demo	• Network Penetration - Demo

Table 8: KBP003 - Contenu du cours - Cyber Security (Meeting#8)

Chapitre	Contenu
Wireless Network penetration-Demo	• John the Ripper/Crunch • Brute-force search / attack • Password cracking/ WPA2 crack
Security Summary	• Policy enforcement • Organization Security personal and hierarchic • Chief Information Security Officer – CISO • Penetration Tester / Hacker • Forensics • Information Security Administrator: ISAD • Information Security Auditor • Application Development Security Expert • InfoSec Systems Project Manager • InfoSec Incident Expert • Physical InfoSec Expert • Behavior Analysis Expert and To-Do-List

Ce sujet continue à la page suivante

KBP003 – Fondements de la cybersécurité et IA, Suite

Contenu du cours, Suite

Table 9: KBP003 - Contenu du cours - AI (Meeting#1)

Chapitre	Contenu
Introduction to AI	• What is AI • AI history • Types of AI • What can we (telecom industry) do with it
Neural networks	• NN networks theory / how it works • Available analytics tools • Real life examples / case study • What can we do with it
Statistic / Social AI	• The crowd is smarter than the Bishop • How it works • Real life examples / case study • What can we do with it

Table 10: KBP003 - Contenu du cours - AI (Meeting#2)

Chapitre	Contenu
NLP - Natural language processing	• What is NLP and how it relates to AI • Natural Language Understanding (NLU) • Natural Language Generation (NLG) • Real life examples / case study • What can we do with it
The future of CRM/CEM	• What will be the interface? • Shortening (and focusing) the session • Predication for CEM • AI for CEM
The End	• Q&A • Course's Evaluation