CATALOGUE DE FORMATION
18/06/2020

KAÏNA-COM
CATALOGUE DE FORMATION

Des menaces au code

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

KSE005 – Des menaces au code

Référence

KSE005

Niveau

- ☒ Débutant
- ☒ Intermédiaire
- ☐ Expert

Nombre de jours

Programme de formation :

- 16 heures (4 heures/jour)

Lieu de la formation

- ☐ I: i-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

Avoir une solide compréhension des réseaux TCP / IP et maîtriser au moins un langage de programmation - C / C ++, C #, PHP, Java ou JavaScript.
Un niveau d'anglais business moyen est requise car la formation sera dispensée en anglais.

Public

Si vous développez des produits logiciels qui se connectent à un réseau - des produits tels que des dispositifs médicaux, des applications SaaS ou des applications médicales mobiles - vous devriez y assister.

Ce sujet continue à la page suivante

KSE005 – Des menaces au code, Suite

Objectifs

«Des menaces au code» est une introduction concentrée et rapide au développement de code sécurisé pour toute l'équipe de développement logiciel, du managers à l'ingénieur d'implémentation. Nous introduisons une approche analytique des menaces basée sur la compréhension des menaces qui comptent vraiment et le deuxième jour, nous nous penchons sur la bonne évaluation de la sécurité logicielle et le codage sécurisé pour atténuer les menaces telles que le Shellcode et les attaques par débordement de tampon.

Ce sujet continue à la page suivante

KSE005 – Des menaces au code, Suite

Contenu du cours

Contenu du cours :

Day #1 - An Introduction to threat modeling and analysis

Table 1: KSE005 - Contenu du cours (Day#1)

Chapter	Description
Ideology	• Why bother modeling? • Why security defenses don't work • Why risk management is broken • Bridging the valley of death between IT and security • A secure SDLC (software development life-cycle) for an unsecure world
Security metrics	• Escaping the hamster wheel of pain • Defining security metrics – What makes a good metric, bad metric, what is not a metric? – Modelers versus measurers
How to measure anything	• Asset valuation • Threat damage to asset • Probability of occurrence
Threat modeling and analysis objectives and drivers	• Qualitative or quantitative? • Is there ROI on security? • Compliance drivers: Industry, Government, Vendor-neutral standards
Threat modeling building blocks	• Threats / attack scenarios • Assets • Vulnerabilities • Countermeasures – Encryption – Network monitoring – Auditing activity logs and data flows – Input validation – Error handling

Ce sujet continue à la page suivante

KSE005 – Des menaces au code, Suite

Contenu du cours, Suite

Chapter	Description
Analyzing your threat model	• Analyzing your threat model and building a cost-effective security countermeasure plan
Pulling it all together	• A class exercise
Software vulnerability fundamentals	• Vulnerabilities – Security Policies – Security expectations • Classifying vulnerabilities – Design vulnerabilities – Implementation vulnerabilities – Operational vulnerabilities – Gray areas • Common threads – Input and data flow – Trust relationships – Assumptions and misplaced trust – Interfaces – Environmental attacks – Exceptional conditions

Ce sujet continue à la page suivante

KSE005 – Des menaces au code, Suite

Contenu du cours, Suite

Day #2 – An Introduction to secure coding

Table 2: KSE005 - Contenu du cours (Day#2)

Chapter	Description
Design review	• Software design fundamentals – Algorithms – Abstraction and decomposition – Trust relationships – Principles of software design – Fundamental design flaws • Enforcing security policy – Authentication – Authorization – Accountability – Confidentiality – Integrity – Availability • Threat modeling of software – Data collection – Attack trees – Prioritizing
Operational review	• Exposure – Attack surface – Insecure defaults – Access control – Unnecessary services – Secure channels – Spoofing – Network profiles • Countermeasures – Development-based – Host-based – Network-based

Ce sujet continue à la page suivante

KSE005 – Des menaces au code, Suite

Contenu du cours, Suite

Chapter	Description
Software vulnerabilities	• Buffer overflows – Process memory layout – Stack overflows – Off-by-one errors – Heap overflows – Global and static data overflows • Shellcode – Writing the code – Finding your code in memory • Protection mechanisms – Stack cookies – Heap hardening – Non-executable stack and help protection • Address space layout – Randomization – SafeSEH – Function pointer obfuscation
Windows objects and the file system	• Processes and threads – Process loading – ShellExecute and ShellExecuteEx – DLL loading – Services • File access – File permissions – File IO API – Links
Windows messaging	• Window messages • Shatter attack

Ce sujet continue à la page suivante

KSE005 – Des menaces au code, Suite

Contenu du cours, Suite

Chapter	Description
Network vulnerabilities in practice	• TCP connections, an overview • TCP streams – TCP spoofing – Connection fabrication – Connection tampering – Blind reset attacks – Blind data injection attacks – TCP segment fragmentation spoofing
The End	• Summary • Q&A • Evaluation