Cybersécurité
La synthèse technique

Introduction

Ransomware, espionnage économique ou scientifique, fuites de données à caractère personnel,… le nombre de cyberattaques ne cesse d'augmenter en France et dans le monde. La question n'est donc pas de savoir si votre organisme sera attaqué mais plutôt comment répondre efficacement à ces attaques. Cette formation, disponible aujourd'hui en e-learning, répond à toutes les préoccupations actuelles et dresse l'état de l'art en matière de cybersécurité à destination des entreprises et des administrations.

Formateur

Boris Motylewski est ingénieur de formation et expert judiciaire en cybercriminalité à la cour d'appel de Montpellier. Il a fondé et dirigé la société ExperLAN, SSII spécialisée dans la sécurité des SI (rachetée par Thalès) puis la société Axiliance, éditeur du pare-feu Web RealSentry (rachetée par Beeware). Il a cofondé la société Securiview, spécialisée dans la détection et remédiation des incidents de sécurité (rachetée par Linkbynet en janvier 2018). Il dirige aujourd'hui la société VeriSafe spécialisée dans la Cybersécurité. Conférencier depuis 1995, Boris Motylewski a formé à ce jour plus de 10 000 professionnels de l'IT (RSSI, DSI, experts cybersécurité, chefs de projet, ingénieurs, auditeurs, consultants, enquêteurs de police judiciaire, DPO, etc…).

A qui s'adresse cette formation ?

Cette formation s'adresse à toute personne désireuse d'acquérir de solides connaissances en matière de cybersécurité. Elle concerne en particulier : DSI, RSSI, architectes, chefs de projets, auditeurs, consultants, enquêteurs de police ou gendarmerie, commerciaux avant-vente, administrateurs IT et développeurs.

Prérequis

Des connaissances générales sur l'informatique et le réseau Internet sont nécessaires pour suivre cette formation. Afin de vous permettre de suivre cette formation avec les meilleures chances de succès, vous pouvez évaluer directement vos connaissances en cliquant sur : https://www.securitecloud.com/formation-cybersecurite-pre-requis/

Durée

Cette formation est réalisée en sessions de formation ouverte à distance (FOAD) également appelé e-learning ou distanciel. La durée totale de la formation est de 20 heures 10 minutes (140 sessions vidéos). Cette durée ne comprend pas le temps passé par les participants aux QCM d'auto-évaluation.

Démonstrations

Des extraits vidéos de cette formation sont disponibles à l'adresse : https://www.certicyber.com/demo

Objectifs pédagogiques

- Appréhender les risques cyber et les enjeux de sécurité
- Identifier les différents composants d'une architecture sécurisée
- Comprendre le rôle et les limites des principales solutions de cybersécurité (Firewall, antivirus, IPS, WAF, etc…)
- Comprendre les principes fondamentaux de cryptographie
- Appréhender les techniques de sécurisation des flux
- Comprendre les attaques applicatives et les mesures de protection associées
- Identifier les points critiques pour la sécurité du cloud, des accès distants et de la mobilité
- Gérer les processus de supervision de la sécurité d'un SI

Méthodes pédagogiques

Présentation magistrale avec analyse technique et déclinaison opérationnelle de tous les points identifiés dans le programme et illustrations concrètes avec de nombreux exemples réels.

Cette formation exclusivement disponible en e-learning est structurée en 10 modules avec pour chaque module :

- Introduction / objectifs
- Contenu pédagogique (le contenu et la durée de chaque module sont détaillés dans le programme de la formation)
- Conclusion / synthèse
- QCM de suivi du module (5 questions)

Durant la formation, les participants peuvent consulter le support de cours comprenant l'ensemble des planches utilisées pour l'animation des différentes sessions vidéos. Dans la version réactualisée en mai 2021, le support comprend 587 slides.

Suivi de la formation & attestation

Cette formation e-learning fait l'objet pour chaque module d'une évaluation de suivi via un QCM de 5 questions. Pour accéder au QCM d'évaluation du module, les participants doivent avoir suivi tous les chapitres de formation du module.

Une attestation de suivi est délivrée à chaque participant ayant effectué l'intégralité des QCM de fin de module.

Evaluation & certification

Chaque participant peut s'auto-évaluer en fin de formation via un QCM de 25 questions portant sur l'ensemble du programme de la formation. Un certificat VERISAFE attestant les compétences acquises est délivré à toute personne ayant obtenu un taux de bonnes réponses supérieur ou égal à 80%.

e-learning 20H

Cybersécurité : synthèse technique

➢ Crypto, HSM, Firewall NG, PKI, IPS, CASB, SOAR, VPN, UEBA, EDR, WAF, SIEM, CTI, SOC 2.0,…

1 Principes fondamentaux & Cybercriminalité

Les principes fondamentaux de la cybersécurité

- La classification CAID (Confidentialité, Auditabilité, Intégrité, Disponibilité)
- Les principes de la SSI : politique de sécurité, défense à profondeur, réduction de la surface d'attaque, moindre privilège
- La gestion des risques et les méthodes MEHARI, EBIOS et ISO 27005

Introduction à la cybercriminalité

- Définir la cybercriminalité
- Cybercriminalité vs Cyberguerre
- Exemples d'opérations cybercriminelles (états, entreprises, OIV et particuliers)
- Le panorama de la cybercriminalité
- Les principaux incidents de sécurité dans le monde et panorama des cyber-attaques (APT, spear phishing, O-day exploit, …)
- Les fuites majeures de données
- Le TOP 15 des menaces cyber selon l'ENISA
- Les principales cyber-attaques en France

Les vulnérabilités logicielles (failles de sécurité)

- l'évolution du nombre de vulnérabilités
- Le cycle de vie des vulnérabilités : de la découverte jusqu'à l'application du correctif
- La gestion des vulnérabilités (Patch management) : Quelle démarche pour une mise en œuvre efficace ?

Les ressources pour la cybersécurité

- Panorama des normes ISO 2700x
- Les principales ressources SSI : ANSSI, NIST, ISO, ENISA, CLUSIF, CSA, …

2 Architectures sécurisées, sécurité de la virtualisation et du cloud

Architecture sécurisée et firewall NG & UTM

- La mise en place de solutions DMZ (zones démilitarisées), DMZ front-office/back-office
- Les solutions intégrées de type UTM avec VPN IPSec, IPS, Content filtering, WAF, …
- Les firewalls NG & UTM (évolutions de l'offre et principaux acteurs)
- Le filtrage des contenus (entrants et sortants), contraintes techniques et juridiques
- Les solutions IPS (Intrusion Prevention System) et IPS NG
- Firewall et proxy : quelle complémentarité ? Proxy vs Reverse proxy

La sécurité de la virtualisation

- Panorama des menaces et vulnérabilités spécifiques à la virtualisation
- Les risques majeurs de la virtualisation : comment y remédier ?
- Les attaques sur tous les composants de la virtualisation
- Les bonnes pratiques pour la sécurité des environnements virtuels et recommandations ANSSI, ENISA et NIST

La sécurité dans le Cloud computing

- Comment identifier, valoriser et traiter les risques dans le Cloud Computing ?
- L'intérêt des offres CASB (Cloud Access Security Broker)
- Normes ISO 27017 & 27018 : quel apport pour la sécurité dans le Cloud ?
- Les 5 façons de vérifier les garanties de sécurité d'un fournisseur
- Les audits de sécurité et tests d'intrusion dans le Cloud
- Les labels de sécurité des fournisseurs
- Les certifications internationales ISO 27001 et SSAE16/ISAE 3402
- Le label de sécurité SecNumCloud de l'ANSSI

3 Notions fondamentales de cryptographie

Principes fondamentaux de cryptographie

- Les techniques cryptographiques pour assurer intégrité et confidentialité, signature électronique et mécanisme de non-répudiation
- Législation et principales contraintes d'utilisation en France et dans le monde
- Les algorithmes à clé publique (Diffie Hellman, RSA) et symétrique (AES, 3DES, RC4,…)
- Les fonctions de hachage (MD5, HMAC, SHA1, SHA2 et SHA3) et la résistance aux collisions
- L'architecture d'une PKI (CA, RA, CPS,…), les certificats (norme X509) et la gestion des révocations (CRL, OCSP)
- Les bonnes pratiques concernant la protection des données via le chiffrement
- Les recommandations de l'ANSSI et de l'ENISA
- Aspects juridiques de la cryptographie

4 Authentification des utilisateurs

Authentification des utilisateurs

- Mot de passe, jeton, carte à puce, smartcard, FIDO, clé USB et puce RFID
- L'authentification biométrique (empreinte digitale, iris, visage,…) et aspects juridiques
- Calcul de la résistance des mots de passe aux attaques par force brute
- Les 5 attaques sur les mots de passe (brute force, sniffing, credential stuffing, keylogger, phishing)
- Les coffres-forts de stockage des mots de passe (Dashlane, keepass, 1password, Lastpass)
- Les systèmes non rejouables OTP (One Time Password), soft token et hard token et l'authentification par carte à puce et certificat client X509
- l'Open Authentication (OATH), les standards HOTP et TOTP, client Google authenticator
- Les standards UAF et U2F de l'alliance FIDO (Fast ID Online)

5 Sécurité des flux réseaux et des accès distants

Le protocole IPsec

- Le standard IPSec, protocoles AH, ESP, IKE et la gestion des clés
- Les recommandations de l'ANSSI pour optimiser la sécurité IPSec

SSL/TLS et HTTPS

- La crypto API SSL/TLS, ses évolutions (de SSL v2 à TLS v1.3) et ses failles.
- Les attaques en interception sur les flux HTTPS (sslsnif, sslstrip), déchiffrement des flux https : aspects juridiques
- Les bonnes pratiques de sécurité HTTPS (certificat EV, HSTS, pinning, CAA, Certificate Transparency,…)
- Le confinement hardware des clés (cartes et appliances HSM), certifications FIPS-140-2 et critères communs
- Comment évaluer facilement la configuration TLS d'un serveur HTTPS ?

Les technologies VPN

- Technologie et produits de VPN SSL et VPN IPsec
- La création d'un VPN (Virtual Private Network) site à site via Internet
- IPSec ou VPN SSL : quel est le meilleur choix pour les postes nomades ?

6 Sécurité des réseaux WiFi

Sécurité WiFi

- Les risques spécifiques au WiFi : Rogue AP, Interception du trafic, redirection, man in the middle, war driving, DoS, …
- Les failles WEP, WPA, WPS et leurs techniques d'exploitation. Comment y remédier ?
- Les failles WPA et WPA2 : Beck-Tews, KRACK
- La sécurité avec WPA3, la norme IEEE 802.11i et les méthodes d'authentification (IEEE 802.1X, EAP-TLS, EAP-TTLS, ...)
- Les bonnes pratiques pour la sécurité des réseaux WLAN

7 Sécurité des postes utilisateurs

La sécurité des postes utilisateurs

- Comprendre toutes les menaces spécifiques aux postes clients : cryptovirus, ver, trojan, backdoor, spyware, adware, scareware, rootkit, 0day,…
- Les logiciels antivirus/antispyware : critères de choix, comparatif et déploiement et les solutions en ligne (Virustotal, Anubis, Malwr, VxStream,…)
- Les failles dans les navigateurs et les attaques de type «drive by download»
- Les rançongiciels : comment y remédier ?
- Le chiffrement des disques durs et des périphériques amovibles (disques externes, clés USB, …)
- Le contrôle de conformité, IEEE 802.1X, Cisco NAC, Microsoft NAP
- Les 3 actions critiques sur un poste utilisateur

8 Mobilité : Smartphones, tablettes, ordinateurs portables et clé USB

Sécurité des portables, tablettes & smartphones

- Panorama des attaques et point sécurité des deux principales plates-formes (iPhone & Android)
- Virus et codes malveillants : quel est le risque réel ? Quel est l'intérêt d'un antivirus ?
- Chiffrement iPhone ou Android : un frein réel pour les enquêtes judiciaires ?
- Les recommandations de sécurité pour les portables, tablettes et smartphones

La problématique des clés USB

- Les risques liés aux clés USB (perte, vol, clé malveillante, …), faille BadUSB, keylogger USB, Rubber Ducky, …
- Les clés USB chiffrées disponibles sur le marché. La solution Microsoft Bitlocker to go
- Les bonnes pratiques d'utilisation des clés USB

9 Sécurité des applications Web

La sécurité applicative

- Comment appliquer le principe de la défense en profondeur pour sécuriser les applications Web en production ?
- Applications Web et mobiles : quelles différences en matière de sécurité ?
- Les dix risques de sécurité des applications : Top Ten OWASP 2017 et les principales attaques : XSS, CSRF, SQL injection, vol de session,…
- Les méthodes de développement sécurisé (SDLC, CLASP, …), la norme ISO 27034 et la méthodologie ASVS de l'OWASP
- Les firewalls applicatifs, aspects techniques et retours d'expérience

L'évaluation de la sécurité des applications

- Les outils de validation de code (SCA)
- Les WASS (Web Application Security Scanning) pour la détection des vulnérabilités
- L'évaluation de la sécurité applicative avec ASVS (Application Security Verification Standard)

10 Audit, test d'intrusion et supervision active de la sécurité

Comment gérer la sécurité au quotidien ?

- Comment construire un tableau de bord Sécurité.
- Les indicateurs de sécurité de l'ETSI

Comment contrôler le niveau de sécurité ?

- Les audits de sécurité et les tests d'intrusion (black box, gray box et white box)
- Comment procéder à une évaluation de sécurité ? Aspects techniques, organisationnels et juridiques
- Les logiciels de scan avancés VDS : Qualys, Nessus, Mandiant, iTrust, …
- Intérêt des plates-formes de « bug bounty » pour identifier les failles de sécurité.
- La veille technologique : comment se tenir informé des nouvelles failles ou vulnérabilités ?

Détection et remédiation des incidents de sécurité

- Le Security Information and Event Management (SIEM) et la gestion centralisée des logs
- Pourquoi et comment mettre en œuvre un SOC (Security Operation Center) ?
- Les référentiels de qualification de l'ANSSI (PASSI, PDIS et PRIS)
- La gestion des incidents de sécurité et les cyber-assurances
- Les évolutions majeures du SOC 2.0