Sommaire

Comment se protéger contre les attaques persistantes ? Page 9
Logiciel d'audit de fichiers : quelles sont les questions à se poser ? Page 9
Sécuriser les systèmes industriels : quelles sont les étapes clés ? Page 9
Attaques DDoS : comment réagir ? Page 10
Sécurité : quelles sont les technologies à connaître ? Page 10
Shadow IT : comment limiter les risques ? Page 11
Qu'est-ce qu'un onduleur ? Page 11
Comment renforcer la robustesse d'un mot de passe ? Page 13
Quelles sont les exigences d'un plan de continuité ? Page 13
Insécurité : quels sont les six risques majeurs ? Page 14
Quelles sont les types d'attaques contre les DNS ? Page 14
Objets connectés : quels sont les points de sécurité à considérer ? Page 15
Quels sont les profils de salariés face aux risques ? Page 15
Comment évaluer les risques d'un système industriel ? Page 15
Identité et contrôle d'accès : quelles sont les quatre approches projets possibles ? Page 16
Qu'est-ce qu'une fédération d'identités ? Page 16
Quels sont les scénarios les plus risqués ? Page 16
Comment éviter la perte de données sur des systèmes virtuels ? Page 17
Comment protéger les données contre les cyber-attaques ? Page 17
Comment élaborer un kit de défense ? Page 17
Quels sont les pires endroits pour stocker ses mots de passe ? Page 18
Comment définir une grille d'analyse de risques ? Page 18
Comptes à privilèges : quelles sont les précautions à prendre ? Page 18
Comment élaborer une grille d'évaluation des risques projets ? Page 19
Quels sont les risques des objets connectés ? Page 19
Quelles sont les différences entre les hackers traditionnels et les hackers étatiques ? Page 20
Quels sont les concepts-clés de la surveillance de la performance du SI ? Page 20
Quel est le scénario d'attaque par ingénierie sociale ? Page 21
Quelles sont les caractéristiques des logiciels malveillants ? Page 21
Quelles sont les étapes du déroulement d'une attaque ? Page 21
Comment définir un plan de sécurité pour le cloud ? Page 22
Quelles sont les péchés capitaux de la sécurité des applications mobiles ? Page 22
Quels sont les sept scénarios catastrophes du BOYD ? Page 22
Quelles sont les causes des pannes logicielles ? Page 23
Quels sont les pièges des solutions de management des informations de sécurité ? Page 23
Quels sont les inconvénients du filtrage de DNS ? Page 23
Quels sont les risques les plus redoutés ? Page 24
Qu'est-ce que le SSO ? Page 24
Comment prévenir les risques liés à la mobilité ? Page 24
Comment les cybercriminels protègent-ils leur anonymat ? Page 25
Quelles sont les menaces qui touchent les bases de données ? Page 25
Quelles sont les caractéristiques d'un plan de reprise d'activités ? Page 25
Quelles sont les caractéristiques des entreprises les mieux protégées ? Page 26
Quelles sont les questions à se poser avant de définir une stratégie de sécurité ? Page 26
Comment gérer les utilisateurs face à la sécurité dans le cloud ? Page 26
Comment sécuriser les développements ? Page 27
Quelles sont les vulnérabilités associées aux objets connectés ? Page 27
Comment organiser les cent premiers jours du RSSI ? Page 27
Qui doit tester la sécurité des applications et quand ? Page 28
Comment savoir si un backup n'est plus à la hauteur ? Page 28
Quels sont les risques les plus redoutés ? Page 28
Qu'est-ce que la cybersécurité ? Page 29

Quelles sont les mauvaises pratiques pour sensibiliser les utilisateurs aux menaces de phishing ? Page 29
Quelles sont les menaces pour les terminaux mobiles ? Page 29
Qu'est-ce qu'une attaque DDoS ? Page 29
Comment combattre la fraude interne ? Page 30
Qu'est-ce qui empêche les RSSI de dormir ? Page 30
Quels sont les points clés de PCI-DSS ? Page 30
Qu'est-ce qu'une attaque DDoS par réflexion ? Page 31
Comment sensibiliser les salariés aux dangers des attaques de phishing ? Page 31
Pourquoi le cloud est plus efficace pour la résilience du système d'information ? Page 32
Quelles sont les étapes pour préparer un audit du système d'information ? Page 32
A qui reportent les RSSI ? Page 32
Quelles sont les erreurs à éviter pour définir une politique de sécurité ? Page 33
Quels sont les signaux faibles liés aux cyber-attaques ? Page 33
Qu'est-ce que le triple A de la sécurité ? Page 33
Quelles sont les indicateurs d'une mauvaise gestion des vulnérabilités ? Page 34
Comment définir la maturité d'une entreprise dans sa réponse aux incidents ? Page 34
Quels sont les aspects à prendre en compte pour la sécurité numérique ? Page 35
Quels sont les types de vulnérabilités et de protection pour les datacenters ? Page 35
Quels sont les principaux risques du Big Data ? Page 36
Quelles sont les principales failles des objets connectés ? Page 36
Quelles sont les recommandations pour sécuriser le cloud ? Page 37
Quelles sont les menaces les plus fréquentes sur les terminaux mobiles ? Page 37
Quels sont les login les plus utilisés par les cybercriminels ? Page 37
Quelles sont les questions que les DG posent aux DSI et aux RSSI ? Page 38
Comment sécuriser une chaîne logistique ? Page 38
Quelles sont les erreurs à éviter pour protéger les données ? Page 38
Quelles sont les bonnes pratiques de sécurité à rappeler aux utilisateurs ? Page 38
Quelles sont les menaces et les solutions pour sécuriser les mobiles ? Page 39
Quelles sont les conséquences des arrêts applicatifs ? Page 39
Comment définir une échelle de maturité de la sécurité ? Page 39
Comment sécuriser un poste de travail ? Page 40
Quels sont les principes à suivre pour récupérer des données en cas de sinistre ? Page 40
Comment se protéger des ransomwares ? Page 41
Quelles sont les précautions à prendre pour se connecter aux réseaux Wi-Fi ? Page 41
Quels sont les principes de base du contrôle d'accès aux applications ? Page 41
Quelles sont les principales sources de vulnérabilités dans les entreprises ? Page 42
Quels sont les principes clés de la réaction sur incident ? Page 42
Comment éviter l'addiction aux bugs ? Page 42
Quels sont les principes de maîtrise des risques dans le cloud ? Page 43
Quels sont les principaux risques de la transformation numérique ? Page 43
Quels sont les éléments de la maturité de la sécurité du SI ? Page 43
Quelles sont les questions à poser à un fournisseur pour protéger les données ? Page 44
Quelles sont les bonnes pratiques pour limiter les risques dans le cloud ? Page 44
Quelles sont les qualités indispensables d'un RSSI ? Page 43
Quels sont les impacts visibles et les impacts cachés des menaces ? Page 45
Comment sécuriser SAP ? Page 45
Quelles sont les mesures à adopter lutter contre des ransomwares ? Page 45

Comment sécuriser une messagerie ? Page 46
Comment sécuriser les terminaux mobiles ? Page 46
Comment sécuriser une démarche DevOps ? Page 46
Quelles solutions utiliser pour se protéger contre les logiciels malveillants ? Page 46
Pourquoi les pirates aiment-ils tant les réseaux ? Page 47
Comment réagir à une attaque ? Page 48
Quelles questions doit-on se poser pour sécuriser un système SAP ? Page 48
Comment combattre les ransomwares ? Page 48
Qu'est-ce qu'un Security Operations Center ? Page 49
Comment parler sécurité au Comex ? Page 49
Quelles sont les règles à respecter pour parler sécurité au Codir ? Page 49
Comment parler de cybersécurité aux membres d'un Comex ? Page 50
Quels sont les domaines à couvrir pour manager les risques ? Page 50
Quels sont les bonnes pratiques pour devenir une organisation résiliente ? Page 50
Quelles sont les fonctionnalités indispensables d'une solution de sauvegarde ? Page 51
Quels est le Top 10 des mots de passe les plus hackés ? Page 51
Quelles sont les questions qu'un DG doit poser à son RSSI ? Page 51
Quels sont les indices à connaître pour prévenir les incidents de sécurité ? Page 52
Quelles sont les composantes d'une gestion des habilitations ? Page 52
Comment se protéger contre les cryptolockers ? Page 52
Comment se diffusent les virus informatiques ? Page 53
Quels sont les pièges à éviter pour un projet IAM ? Page 53
Quelles sont les mesures à prendre pour se défendre contre ransomwares ? Page 53
Quels sont les éléments à surveiller pour sécuriser les données ? Page 53
Pourquoi faire appel à un prestataire de sécurité ? Page 54
Quelles les sont les faiblesses des systèmes industriels ? Page 54
Quelles sont les principales causes des bugs ? Page 54
Quelles sont les contraintes pour sécuriser un système Scada ? Page 54
Quels sont les facteurs clés de succès pour sécuriser les terminaux mobiles ? Page 55
D'où proviennent les failles des terminaux mobiles ? Page 55
Quel est le temps d'interruption après une attaque ? Page 55
Pourquoi faut-il sécuriser les réseaux locaux ? Page 56
Comment se prémunir des ransomwares ? Page 56
Comme limiter les risques liés à l'IoT ? Page 56
Comment sensibiliser les utilisateurs à la sécurité ? Page 56
Comment se défendre contre la fraude au président ? Page 57
Quelles sont les vulnérabilités les plus fréquentes avec les objets connectés ? Page 57
Quelles sont les familles de métiers dans la sécurité ? Page 57
Quels réflexes de cyber-hygiène faut-il adopter ? Page 58
Quels sont les facteurs de risques de l'ingénierie sociale ? Page 58
Quels sont les points d'attention à considérer pour les contrôle d'accès ? Page 58
Quelle est l'évolution historique des budgets sécurité ? Page 59
Pourquoi attaquer un terminal mobile ? Page 59
Comment un mobile peut-il être attaqué ? Page 60
Quelles sont les priorités sécurité des entreprises pour 2018-2020 ? Page 60
Quelles sont les conséquences des cyber-attaques sur l'activité des entreprises ? Page 61
Quelles sont les conseils à suivre pour sécuriser les réseaux ? Page 61

Comment bien se défendre contre les ransomwares ? Page 61
Quelles sont les meilleures approches pour se protéger ? Page 62
Quelles sont les impacts visibles et invisibles de l'insécurité IT ? Page 62
Comment renforcer une architecture de sécurité ? Page 62
Quelles sont les garanties à prévoir pour sécuriser les objets connectés ? Page 63
Dans quelle mesure le marché de la cybersécurité est-il porteur ? Page 63
Quels sont les chantiers les plus difficiles du RGPD ? Page 64
Quelles sont les raisons d'utiliser une authentification forte ? Page 64
Quels sont les objectifs d'une gestion de crise ? Page 64
Comment protéger les environnements Office 365 ? Page 65
Comment mener un projet de Bug Bounty ? Page 65
Quelles sont les mauvaises habitudes des entreprises après un piratage de données ? Page 66
Quelles sont les principales menaces de sécurité ? Page 66
Quelles sont les composantes d'une stratégie sécurité ? Page 67
Quelles sont les bonnes pratiques de la gestion des accès et des identités ? Page 68
Comment découper un SI en zones de confiance ? Page 68
Quel est le Top 15 des pires mots de passe des utilisateurs ? Page 69
Comment sécuriser des applications mobiles ? Page 69
Qu'est-ce que la gestion des accès et des identités ? Page 69
Quels sont les mythes du phishing ? Page 70
Quelles questions faut-il poser aux prestataires de sauvegarde dans le cloud ? Page 70
Quelles sont les caractéristiques du risque cyber ? Page 70
Quelles sont les mauvaises pratiques de la gestion des accès et des identités ? Page 71
Quels sont les fondamentaux de la sensibilisation à la sécurité ? Page 71
Comment réagir à un incident réseau ? Page 71
Pourquoi les fichiers de logs ne suffisent pas dans le cloud ? Page 72
Quelles sont les questions à se poser concernant les mots de passe administrateur ? Page 72
Quels sont les malwares les plus actifs en France ? Page 73
Quelles sont les étapes d'un test d'intrusion ? Page 73
Quels sont les ingrédients d'une sécurité de bout en bout ? Page 73
Quelles sont les sources de vulnérabilités des ERP ? Page 74
Comment pirater un fax ? Page 74
Quels sont les avantages d'un système d'information de gestion des risques ? Page 75
D'où viennent les incidents réseaux ? Page 75
Datacenters : quelles sont les causes de pannes ? Page 76
Charte d'utilisation des moyens nformatiques : quels points clés ? Page 76
Cybersécurité : quels sont les points de vigilance ? Page 76
Sécurité : un marché mondial tiré par les services et les infrastructures Page 77
Gestion des identités : quels sont les trois défis à gérer ? Page 77
Quelles priorités pour un nouveau RSSI ? Page 77
Contrôle d'accès : quelles sont les erreurs les plus courantes ? Page 78
Quelles sont les vulnérabilités non techniques du cloud ? Page 78
Sécurité : quels sont les points faibles ? Page 78
Sécurité : quelles sont les sept tendances du futur ? Page 78
Combien gagnent les professionnels américains de la sécurité ? Page 79
Ressources en cybersécurité : la pénurie affecte-t-elle la performance ? Page 79
Comment se diffusent les ransomwares ? Page 79
Architectes sécurité : quelles compétences ? Page 79
Quel est le Top 5 des risques pour les PME ? Page 79
Quelles sont les missions d'un RSSI ? Page 80
Quels sont les différents types de ransomwares ? Page 80
Cybersécurité : comment faire une check-list ? Page 80

Quels sont les principaux risques du cloud ? Page 81
Campagne de phishing : comment faire ? Page 81
Cyber-attaques : quels sont les cinq axes stratégiques pour se protéger ? Page 81
Sécurité des réseaux industriels et objets connectés : quelles bonnes pratiques ? Page 82
Quelles sont les attaques subies par les grandes entreprises françaises ? Page 82
Sécurité des données dans le cloud : quels sont les principes à retenir ? Page 82
Incident de sécurité : que faire ? Page 83
Quelles sont les priorités stratégiques pour la cybersécurité ? Page 83
Comment se protéger contre les principaux malwares ? Page 83
Pourquoi la protection des données person-nelles allonge les cycles de vente ? Page 84
Attaque via le cloud : quel scénario pour quel impact ? Page 84
IoT : quels sont les points d'attention ? Page 84
Sécurité : quelles sont les cinq erreurs les plus communes ? Page 85
Les hackers font-ils moins peur que les araignées ? Page 85
Risque fournisseur : quelles sont les six étapes pour se protéger ? Page 85
E-mails frauduleux : quel est le Top 10 des mots-clés ? Page 85
Cyber-résilience : quels points-clés ? Page 86
Sécurité des API : quelles sont les cinq questions à se poser ? Page 86
Quelles sont les principales caractéristiques du DevSecOps ? Page 86
Gestion des risques : quelles caractéristiques pour les indicateurs ? Page 86
Quels sont les critères pour bien choisir une technologie réseau ? Page 87
Sécurité : quelles sont les dix règles à appliquer dans l'entreprise ? Page 87
Quels sont les huit traits de personnalité pour réussir dans la cybersécurité ? Page 87
Qu'est-ce que l'API WebAuthn ? Page 88
Quels sont les coûts des incidents informatiques ? Page 88
Quelles sont les onze catégories de cybermenaces ? Page 88
Cybersécurité : quels sont les profils les plus à risque ? Page 89
Quand fraude-t-on le plus ? Page 89
Quels sont les principaux risques du serverless ? Page 89
Prestataires cloud et sécurité : quelles sont les dix attentes des DSI ? Page 90
Cyberattaque : quelles sont les cinq étapes ? Page 90
Cybersécurité et cours de bourse : quels liens ? Page 90
Qu'est-ce que le risque informatique et la cybersécurité ? Page 90
Sécurité : quels sont les ingrédients d'une stratégie de gamification réussie ? Page 91
Cyberattaques : quels sont les secteurs les plus touchés ? Page 91
Extracteurs de cryptomonnaie : un risque sous-estimé ? Page 92
Cybersécurité : quels sont les principaux facteurs de risques ? Page 92
Quel est le coût coûts des incidents de sécurité ? Page 92
Gestion des identités : quels sont les huit points faibles ? Page 93
Risque cyber et risque industriel : quelles différences ? Page 93
Sécurité des données : que redoutent les Français ? Page 93
Cloud public : quelles sont les quatre principales menaces ? Page 93
Quels sont les types de fraude dont sont victimes les entreprises ? Page 94
Sécurité : comment faire du Storytelling ? Page 94
Quels sont les 10 risques les plus redoutés par les entreprises françaises ? Page 94
Comment sécuriser les communications et les données mobiles ? Page 95
Sécurité: combien faut-il dépenser ? Page 96
Qu'est-ce qu'un CERT et un SOC ? Page 96
Phishing et ransomwares : quelles sont les trois questions à se poser ? Page 96
Quelles sont les cinq erreurs les plus courantes ? Page 97
Quelles compétences doivent avoir les DPO ? Page 97
2019, année des vaporworms ? Page 97