

# Sommaire

Introduction .....	11
<b>Chapitre 1 - Les principes .....</b>	<b>15</b>
Le premier piratage de l'histoire.....	15
L'alignement fatal .....	23
Les trois facteurs à maîtriser .....	25
<b>Chapitre 2 - Les menaces, les vulnérabilités, les impacts .....</b>	<b>29</b>
Les menaces exogènes.....	29
Les menaces endogènes .....	34
Les vulnérabilités.....	40
Les impacts .....	45
<b>Chapitre 3 - Les méthodologies.....</b>	<b>53</b>
Les référentiels de contrôles .....	53
Les 9 principes immuables.....	56
Comment s'organiser .....	78
Les 42 règles d'hygiène informatique de l'ANSSI : un point de départ pragmatique .....	80
ISO 27001 : entre prestige de la certification et réalité documentaire .....	84
NIST CSF 2.0 : l'architecture sans prescription .....	88
Pourquoi ce livre s'appuie sur le NIST CSF 2.0 et comment l'utiliser .....	92
<b>Chapitre 4 - Identifier .....</b>	<b>99</b>
Cartographier un territoire qui change pendant que vous le dessinez ....	99
Identifier vos actifs (ID.AM).....	106
Identifier vos risques (ID.RA) .....	122

Améliorer votre posture de gestion du risque (ID.IM).....	146
L'essentiel à comprendre .....	157
<b>Chapitre 5 - Gouverner .....</b>	<b>161</b>
Décider dans le brouillard en espérant y voir clair .....	161
Contexte organisationnel (GV.OC).....	166
Stratégie et gestion des risques (GV.RM).....	176
Rôles, responsabilités et autorités (GV.RR).....	188
Politique (GV.PO) .....	197
Surveillance (GV.OV).....	202
Gestion des risques de la chaîne d'approvisionnement en cybersécurité.....	209
L'essentiel à comprendre .....	225
<b>Chapitre 6 - Protéger .....</b>	<b>229</b>
Construire des murs en sachant qu'ils seront franchis.....	229
Gérer le contrôle des accès (PR.AA) .....	235
Sensibilisation et formation (PR.AT) .....	245
Sécurité des données (PR.DS).....	250
Sécurité de l'infrastructure (PR.PS).....	257
La résilience (PR.IR) .....	266
L'essentiel à comprendre .....	272
<b>Chapitre 7 - Détecter.....</b>	<b>277</b>
Chercher l'aiguille en sachant qu'elle ressemble au foin .....	277
Surveillance (DE.CM).....	284
Analyse des événements (DE.AE) .....	292
L'essentiel à comprendre .....	299
<b>Chapitre 8 - Répondre.....</b>	<b>303</b>
Éteindre l'incendie pendant qu'il se propage.....	303
Gestion des incidents (RS.MA).....	309
Analyse des incidents (RS.AN).....	314
Communiquer (RS.CO).....	319
Mitiger les impacts (RS.MI) .....	321
L'essentiel à comprendre .....	324

---

<b>Chapitre 9 - Récupérer .....</b>	<b>329</b>
Reconstruire sur des ruines en espérant que le sol est stable.....	329
Exécuter le plan de reprise (RC.RP) .....	334
Communiquer après la reprise (RC.CO).....	340
L'essentiel à comprendre .....	343
<b>Chapitre 10 - Construire votre propre stratégie .....</b>	<b>347</b>
Ce que vous devez avoir en tête.....	347
Les 5 phases pour construire votre stratégie.....	356
Glossaire.....	369
À propos de l'auteur.....	379