



SOMMAIRE

| | |
|---|------------|
| INTRODUCTION | 5 |
| CHAPITRE 1 CONFIGURATION DES SYSTÈMES DE DÉTECTION D'INCIDENTS | 9 |
| CHAPITRE 2 QUALIFICATION DES INCIDENTS DE SÉCURITÉ | 19 |
| CHAPITRE 3 PRÉSERVATION DES PREUVES NUMÉRIQUES | 29 |
| CHAPITRE 4 COLLABORATION DANS LA RÉPONSE À INCIDENT | 39 |
| CHAPITRE 5 RÉALISATION D'UN RETOUR D'EXPÉRIENCE | 49 |
| CHAPITRE 6 MISE À JOUR DES RÈGLES DE DÉTECTION SELON LA VEILLE | 57 |
| CHAPITRE 7 SUPERVISION DES INCIDENTS MAJEURS DE SÉCURITÉ | 65 |
| CHAPITRE 8 GESTION DES JOURNAUX D'ÉVÉNEMENTS | 75 |
| CHAPITRE 9 APPLICATION DES MESURES DE RÉPONSE RAPIDE | 83 |
| CHAPITRE 10 COMMUNICATION AVEC LES ANALYSTES CYBER | 93 |
| CHAPITRE 11 PRÉPARATION DES COMPTES RENDUS D'INCIDENTS | 101 |
| CHAPITRE 12 EVALUATION CONTINUE DE L'EFFICACITÉ DES DISPOSITIFS | 107 |
| CONCLUSION | 115 |