



Mémoire de fin d'études

Pour l'obtention du diplôme Post-Graduation Spécialisée Année

Option : Sécurité d'Information

2015/2016

Thème

Etude de la méthode OCTAVE : Application sur un cas pratique

- Membre de Jury :
 - La Présidente : Mme. F. BESSAI
 - L'examineur 1 : M. SAIDI Ahmed
 - L'examineur 2 : M. KHMISSA Hamza

- Proposé par :

Pr. CHALAL Rachid

- Présenté par :

Mr. BOUCHAREB Mourad

CERIST@2016

Promotion: 2015/2016

Résumé

De nombreuses méthodes d'analyse des risques existent dans la littérature comme dans la pratique. Ces méthodes, et malgré qu'elles partagent le même but, ont des visions très différentes sur comment atteindre ce but et donc abordent le problème du risque différemment. Pendant que certaines méthodes traitent tous types de risques, d'autres ne peuvent être appliqués que sur un type de risque bien particulier.

L'objectif de notre travail est d'étudier et d'appliquer la méthode OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) développée par SEI (Software Engineering Institute) de l'université Carnegie Mellon aux USA, sur un cas pratique **SCADA (surveillance, contrôle et acquisition de données)**. Il s'agit d'analyser, sur le plan pratique, cette méthode.

Mots clés :

Analyse des risques, Sécurité des systèmes d'information, Analyse des risques de sécurité des systèmes d'information, Méthodes d'analyse des risques.

Tables des matières

1	Chapitre 1 : Gestion des risques.....	3
1.1	Introduction.....	3
1.2	Terminologie du domaine.....	3
1.3	Le processus de la gestion des risques	5
1.4	L'appréciation des risques de sécurité des SI :	11
1.4.1	Définition de l'appréciation des risques de sécurité des SI :	11
1.4.2	Techniques d'appréciation des risques : Quantitatives Vs Qualitatives	12
1.4.3	Analyse des risques:.....	13
1.4.4	Evaluation des risques:.....	17
1.5	Conclusion :	9
2	Chapitre 2 : Gestion de sécurité des systèmes d'information	10
2.1	Introduction:.....	10
2.2	Définitions:	10
2.2.1	Système d'information :	10
2.2.2	Sécurité des systèmes d'information:	10
2.2.3	Objectifs de sécurité des SI:	11
2.3	L'appréciation des risques de sécurité des SI	11
2.3.1	Définition de l'appréciation des risques de sécurité des SI	11
2.3.2	Technique d'appréciation des risques de sécurité des SI	12
2.3.3	Analyse des risques	13
2.3.4	Evaluation des risques	17
2.4	Conclusion	18
3	Chapitre 3 La méthode OCTAVE	19
3.1	Introduction	19
3.2	Famille de processus CERT® OCTAVE®	19
3.3	La methode OCTAVE-Allegro	20
4	Chapitre 4: Etude de cas	33
4.1	Description de l'infrastructure d'information essentielle	33
4.2	Étape 1 - Établir des critères de mesure du risqué	34
4.3	Étape 2 - Actifs de développement d'informations de profil	38
4.4	Étape 3 - Identifier les Biens d'informations Contenants	41
4.5	Étape 4 – Identifier les préoccupations	43
4.6	Étape 5 – Identifier les scénarios de menace	43
4.7	Étape 6 - Identifier les risques	49
4.8	Étape 7 - Analyser les risques	49
4.9	Étape 8 - Sélectionnez et choisir une Approche face aux risques	55
5	Conclusion de l'Analyse de risque	59
6	Conclusion générale	60