OFFRE PECB



PECB est un fournisseur mondial de services de formation, d'examen et de certification, qui offre son expertise dans de nombreux domaines, notamment la sécurité de l'information, les technologies de l'information, la continuité des activités, le management des services, le management des risques, le management de la qualité, la sécurité, l'environnement, la santé, etc.

PECB est accréditée selon la norme ISO/IEC 17024 par :

- International Accreditation Service (IAS)
- United Kingdom Accreditation Service (UKAS)

PECB fournit à travers ses partenaires des services de formation et certification des professionnels dans les domaines du management de la Qualité, Santé & Sécurité, Environnement, Sécurité de l'Information, Continuité d'Activité, Gestion de service des TI, Sécurité Alimentaire, Gestion d'actifs, Gestion énergétique, Appareils médicaux, et Sécurité de la chaîne d'approvisionnement (accrédité selon la norme ISO/IEC 17021).

L'ISATIC applique les frais de licence par cours et par territoire de PECB. Les formations professionnelles sont basées sur les normes ISO ou d'autres référentiels.

FORMATION ET CERTIFICATION INDIVIDUELLE

Type de	<u>Identification</u>	<u>Durée</u>	<u>Coût</u>
cours		<u>(jour)</u>	(FCFA)
Cours A	Formation + Attestation d'achèvement de formation [ACC]	1	220 000
Cours B	Formation + Examen + Attestation d'achèvement de formation [ACC] + certification	2	450 000
Cours C	Formation + Examen +Attestation d'achèvement de formation [ACC] + certification	3	745 000
Cours D	Formation + Examen + Attestation d'achèvement de formation [ACC] + certification	4	850 000
Cours E	Formation + Examen +Attestation d'achèvement de formation [ACC] + certification	5	950 000

SIX NIVEAUX POUR CHAQUE COURS DE FORMATION LIÉ À LA NORME ISO

1. INTRODUCTION

Une formation d'une journée

2. FONDATION

Une formation de deux jours

3. RESPONSABLE DE LA MISE EN ŒUVRE (LEAD IMPLEMENTER)

Une formation de cinq jours

4. AUDITEUR PRINCIPAL (LEAD AUDITOR)

Une formation de cinq jours

5. **MANAGER**

Une formation de trois jours

6. LEAD MANAGER

Une formation de cinq jours

Programme de formation PECB

<u>N°</u>	<u>Sécurité de l'information</u>	<u>Durée</u> (jour)	<u>Coût</u> (FCFA)
1	ISO/IEC 27001 Introduction: Jour 1: Introduction aux concepts du Système de	1	220 000
	Management de la sécurité de l'information (SMSI), tels que définis par la norme		
	ISO /CEI 2700		
	<u>Prérequis</u> : Aucun		
2	PECB Certified ISO/IEC 27001 Foundation :	2	450 000
	Jour 1 : Introduction aux concepts du Système de management ; de la sécurité de		
	l'information (SMSI), tels que définis par la norme ISO/CEI 27001		
	Jour 2 : Exigences relatives au Système de management de la sécurité de		
	l'information et examen de certification.		

	Próreguis : Augus		
	<u>Prérequis :</u> Aucun <u>Certification :</u> Après avoir réussi l'examen, les participants peuvent postuler		
	à la certification « PECB Certified ISO/CEI 27001 Foundation ».		
	Pour plus d'informations concernant les certifications ISO/CEI.		
3	PECB Certified ISO/IEC 27001 Lead Auditor:	5	950 000
3)	930 000
	Jour 1 Introduction au système de management de la sécurité de l'information		
	(SMSI) et à ISO/IEC 2700		
	Jour 2 Principes d'audit, préparation et initiation d'un audit		
	Jour 3 Activités d'audit sur site		
	Jour 4 Clôture de l'audit		
	Jour 5 Examen de certification		220.000
4	ISO/IEC 27002 Sécurité de l'information - Code de bonne pratique pour le	1	220 000
	management de la sécurité de l'information		
	<u>Jour 1</u> : Introduction aux mesures de sécurité de l'information, telles que définies		
	par la norme ISO/CEI 27002		
	Prérequis : Aucun		
5	PECB Certified ISO/CEI 27002 Foundation	2	450 000
	<u>Jour 1</u> : Introduction à la norme ISO/CEI 27002 et au Système		
	de management de la sécurité de l'information		
	<u>Jour 2</u> : Mesures ISO/CEI 27002 et examen de certification		
	<u>Prérequis</u> : Aucun		
	<u>Certification</u> :		
6	DECD Contified ISO/IEC 27002 Load Manager	5	950 000
6	PECB Certified ISO/IEC 27002 Lead Manager	5	950 000
	Jour 1 Introduction aux mesures de sécurité de l'information conformes à la		
	norme l'ISO/CEI 27002		
	<u>Jour 2</u> Exigences et objectifs de la sécurité de l'information conforme à la norme		
	ISO/CEI 27002		
	<u>Jour 3</u> Surveiller, mesurer, analyser et évaluer les mesures de la sécurité de		
	l'information		
	Jour 4 Amélioration continue de la performance du Système de management de		
	la sécurité de l'information de l'organisation		
	<u>Jour 5</u> Examen de certification		
7	Formations aux méthodes d'appréciation des risques		
	EBIOS	3	745 000
	Jour 1 Objectifs et structure du cours ; Introduction à la méthode EBIOS		
	<u>Jour 2</u> h Atelier 3 « Scénarios stratégiques » ; h Atelier 4 « Scénarios		
	opérationnels »		
	Jour 3 Examen final		
	PECB Certified MEHARI Risk Manager	3	745 000
	Jour 1 Introduction aux concepts et aux étapes de la méthode d'analyse de risque		7-3 000
	MEHARI		
	Jour 2 Conduire une analyse de risque en utilisant la méthode MEHARI		
	Jour 3 Planification de la sécurité selon la méthode MEHARI et examen de		
	certification		
8	ISO/IEC 27005 - Gestion des risques liés à la sécurité de l'information		
	Jour 1 : Introduction aux fondamentaux de la gestion des risques liés à la sécurité		
	de l'information en utilisant la norme ISO/CEI 27005		
	Préreguis : Aucun		
9	PECB Certified ISO/CEI 27005 Foundation	3	745 000
	Jour 1 : Introduction aux concepts fondamentaux de la gestion des risques liées à		
	la sécurité de l'information en utilisant la norme ISO/CEI 27005		
	Jour 2 : Approches de gestion des risques liés à la sécurité de l'information et		
	examen de certification		
		l	

PECB Certified ISO/IEC 27005 Risk Manager Jour 1 Introduction au programme de gestion des risques conforme à ISO/IEC 27005 Jour 2 Mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 27005 Jour 3 Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'Information et examen de certification ISO/IEC 27035 - Gestion des incidents de sécurité de l'Information et examen de certification ISO/IEC 27035 - Gestion des incidents de sécurité de l'Information et examen de certification ISO/IEC 27035 - Introduction aux concepts et aux principes de la gestion des incidents de sécurité de l'Information, tels que définis par la norme ISO/CEI 27035 Préreauis : Aucun Jour 1 : Introduction aux principes et concepts fondamentaux de la gestion des incidents de la sécurité de l'Information, tels que définis par la norme ISO/CEI 27035 Jour 2 : Approches processus de gestion des incidents de la sécurité de l'Information, tels que définis par l'ISO/IEC 27035 Jour 2 : Approches processus de gestion des incidents de la sécurité de l'Information et examen de certification Préreauis : Aucun Certification : PECB Certified ISO/IEC 27035 Lead Incident Manager Jour 1 Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'Information Jour 2 Conception et préparation d'un plan de gestion des incidents de sécurité de l'Information Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'Information Jour 3 Examen de certification 11 Formations en sécurité des ressources humaines PECB Certified Human Ressources Security Foundation Jour 2 : Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Préreauis : Aucun Certification : Cybersécurité 1 ISO/IEC 27032 Formation ISO/IEC 127032 Lead Cybersecurity Manager Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordin		Pué va avida y Avia va		
PECB Certified ISO/IEC 27005 Risk Manager Jour 1 Introduction au programme de gestion des risques conforme à ISO/IEC 27005 Jour 2 Mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 27005 Jour 3 Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification 10 ISO/IEC 27035 - Gestion des incidents de sécurité de l'Information ISO/IEC 27035 Introduction Jour 1: Introduction aux concepts et aux principes de la gestion des incidents de sécurité de l'information, tels que définis par la norme ISO/CEI 27035 Perfequis : Aucun PECB Certified ISO/CEI 27035 Foundation Jour 2: Introduction aux principes et concepts fondamentaux de la gestion des incidents de la sécurité de l'information, tels que définis par la norme ISO/CEI 27035 Jour 2: Approches processus de gestion des incidents de la sécurité de l'information et examen de certification Perfequis : Aucun Certification: PECB Certified ISO/IEC 27035 Lead Incident Manager Jour 1 Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/CEI 27035 Jour 2 Conception et préparation d'un plan de gestion des incidents de sécurité de l'information, tels que définis par l'ISO/CEI 27035 Jour 2 Conception et préparation d'un plan de gestion des incidents de sécurité de l'information de l'information Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de s'écurité de l'information Jour 5 Examen de certification 11 Formations en sécurité des ressources humaines pec pec peut de l'information Jour 5 Examen de certification 12 Expersécurité 13 ESO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2 Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail perfequis : Aucun Certification: Cybersécurité 1 ISO/IEC 27032 Fo		Prérequis : Aucun		
Jour 1 Introduction au programme de gestion des risques conforme à ISO/IEC 27005 Jour 2 Mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 27005 Jour 3 Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification		<u>Certification</u> :		
Jour 1 Introduction au programme de gestion des risques conforme à ISO/IEC 27005 Jour 2 Mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 27005 Jour 3 Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification		PECR Certified ISO/IEC 27005 Risk Manager		
27005 Jour 2 Mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 27005 Jour 3 Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification ISO/IEC 27035 - Gestion des incidents de sécurité de l'information ISO/ELI 27035 Introduction aux concepts et aux principes de la gestion des incidents de sécurité de l'information, tels que définis par la norme ISO/CEI 27035 Prérequis : Aucun PECB Certified ISO/CEI 27035 Foundation Jour 1 : Introduction aux principes et concepts fondamentaux de la gestion des incidents de la sécurité de l'information, tels que définis par la norme ISO/CEI 27035 Jour 2 : Approches processus de gestion des incidents de la sécurité de l'information et examen de certification Prérequis : Aucun Certification : PECB Certified ISO/IEC 27035 Lead Incident Manager Jour 1 Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/CEI 27035 Jour 2 : Conception et préparation d'un plan de gestion des incidents de sécurité de l'information et examen de certification Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 4 Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information Jour 5 Examen de certification 10 Formations en sécurité des ressources humaines PECB Certified Human Ressources Security Foundation Jour 1 : Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2 : Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis : Aucun Certification : Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification			3	745 000
Jour 2 Mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 27005 Jour 3 Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification				743 000
27005 Jour 3 Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification 10 ISO/IEC 27035 - Gestion des incidents de sécurité de l'information ISO/IEC 27035 - Gestion des incidents de sécurité de l'information ISO/IEC 27035 - Gestion des incidents de sécurité de l'information Jour 1: Introduction aux concepts et aux principes de la gestion des incidents de sécurité de l'information, tels que définis par la norme ISO/CEI 27035 Prérequis: Aucun PEGB Certified ISO/IEC 27035 Foundation Jour 1: Introduction aux principes et concepts fondamentaux de la gestion des incidents de la sécurité de l'information, tels que définis par la norme ISO/CEI 27035 Jour 2: Approches processus de gestion des incidents de la sécurité de l'information et examen de certification Prérequis: Aucun Certification: PEGB Certified ISO/IEC 27035 Lead Incident Manager Jour 1 Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information d'un plan de gestion des incidents de sécurité de l'information Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 4 Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information Jour 5 Examen de certification 11 Formations en sécurité des ressources humaines PEGB Certified Human Ressources Security Foundation Jour 1: Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2: Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis : Aucun Crtification : Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour				
Jour 3 Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification ISO/IEC 27083 - Gestion des incidents de sécurité de l'information ISO/IEC 27083 - Gestion des incidents de sécurité de l'information ISO/IEC 27035 Introduction Iso/IEC 27035 Introduction Iso/IEC 27035 Introduction aux concepts et aux principes de la gestion des incidents de sécurité de l'information, tels que définis par la norme ISO/CEI 27035 Prérequis : Aucun PECB Certified ISO/IEC 27035 Foundation Jour 1 : Introduction aux principes et concepts fondamentaux de la gestion des incidents de la sécurité de l'information et examen de certification Prérequis : Aucun Certification : PECB Certified ISO/IEC 27035 Lead Incident Manager Jour 1 Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/CEI 27035 Jour 2 : Conception et préparation d'un plan de gestion des incidents de sécurité de l'information Jour 3 I ancement d'un processus de gestion des incidents de sécurité de l'information Jour 3 I ancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 3 I ancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 5 Examen de certification 11 Permations en sécurité des ressources humaines PECB Certified Human Ressources Security Foundation Jour 5 Examen de certification 12 So/IEC 27032 Formation SO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2 : Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis : Aucun Certification So/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et c				
Information et examen de certification ISO/IEC 27035 - Gestion des incidents de sécurité de l'information ISO/IEC 27035 Introduction 1 220 000 1 20 000 1 20 000 20 2				
1 SO/IEC 27035 - Gestion des incidents de sécurité de l'information So/CEI 27035 Introduction So/CEI 27035 Introduction aux concepts et aux principes de la gestion des incidents de sécurité de l'information, tels que définis par la norme ISO/CEI 27035 Prérequis : Aucun PECB Certified ISO/CEI 27035 Foundation Jour 1 : Introduction aux principes et concepts fondamentaux de la gestion des incidents de la sécurité de l'information, tels que définis par la norme ISO/CEI 27035 Jour 2 : Approches processus de gestion des incidents de la sécurité de l'information et examen de certification Prérequis : Aucun Certification :				
ISO/CEI 27035 Introduction Jour 1 : Introduction aux concepts et aux principes de la gestion des incidents de sécurité de l'information, tels que définis par la norme ISO/CEI 27035 Prérequis : Aucun PFCB Certified ISO/CEI 27035 Foundation Jour 1 : Introduction aux principes et concepts fondamentaux de la gestion des incidents de la sécurité de l'information, tels que définis par la norme ISO/CEI 27035 Jour 2 : Approches processus de gestion des incidents de la sécurité de l'information et examen de certification Prérequis : Aucun Certification : PECB Certified ISO/IEC 27035 Lead Incident Manager Jour 1 Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information Jour 3 Lancement d'un processus de gestion des incidents de sécurité de l'information Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 4 Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information Jour 5 Examen de certification Jour 5 Examen de certification Jour 5 Examen de certification Securité des ressources humaines PECB Certified Human Ressources Security Foundation Jour 1 : Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2 : Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis : Aucun Certification So/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification	10			
Jour 1 : Introduction aux concepts et aux principes de la gestion des incidents de sécurité de l'information, tels que définis par la norme ISO/CEI 27035			1	220 000
sécurité de l'information, tels que définis par la norme ISO/CEI 27035 Prérequis: Aucun PECB Certified ISO/CEI 27035 Foundation Jour 1: Introduction aux principes et concepts fondamentaux de la gestion des incidents de la sécurité de l'information, tels que définis par la norme ISO/CEI 27035 Jour 2: Approches processus de gestion des incidents de la sécurité de l'information et examen de certification Prérequis: Aucun Certification: PECB Certified ISO/IEC 27035 Lead Incident Manager Jour 1 Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/CEI 27035 Jour 2 Conception et préparation d'un plan de gestion des incidents de sécurité de l'information Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 4 Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information Jour 5 Examen de certification 10 Formations en sécurité des ressources humaines PECB Certified Human Ressources Security Foundation Jour 1: Introduction aux concepts fondamentaux de la sécurité des ressources humaines et les qu'exigés par ISO/IEC 27001 Jour 2 : Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis : Aucun Certification: Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification				
Prérequis : Aucun PECB Certified ISO/CEI 27035 Foundation Jour 1 : Introduction aux principes et concepts fondamentaux de la gestion des incidents de la sécurité de l'information, tels que définis par la norme ISO/CEI 27035 Jour 2 : Approches processus de gestion des incidents de la sécurité de l'information et examen de certification Prérequis : Aucun Certification : PECB Certified ISO/IEC 27035 Lead Incident Manager Jour 1 Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/CEI 27035 Jour 2 Conception et préparation d'un plan de gestion des incidents de sécurité de l'information Jour 3 Lancement d'un processus de gestion des incidents de sécurité de l'information Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 5 Examen de certification 10 Jour 5 Examen de certification Prérequis : Aucun Certification : Cybersécurité 1 ISO/IEC 27032 Formation ISO/IEC 17032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification				
PECB Certified ISO/CEI 27035 Foundation Jour 1: Introduction aux principes et concepts fondamentaux de la gestion des incidents de la sécurité de l'information, tels que définis par la norme ISO/CEI 27035 Jour 2: Approches processus de gestion des incidents de la sécurité de l'information et examen de certification Prérequis : Aucun Certification : PECB Certified ISO/IEC 27035 Lead Incident Manager Jour 1 Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/CEI 27035 Jour 2 Conception et préparation d'un plan de gestion des incidents de sécurité de l'information Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 4 Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information Jour 5 Examen de certification 11 Pormations en sécurité des ressources humaines PECB Certified Human Ressources Security Foundation Jour 1: Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2 : Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis : Aucun Certification : Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification				
incidents de la sécurité de l'information, tels que définis par la norme ISO/CEI 27035 Jour 2 : Approches processus de gestion des incidents de la sécurité de l'information et examen de certification Prérequis : Aucun Certification : PECB Certified ISO/IEC 27035 Lead Incident Manager Jour 1 Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/CEI 27035 Jour 2 Conception et préparation d'un plan de gestion des incidents de sécurité de l'information Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 5 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 5 Examen de certification 11 Formations en sécurité des ressources humaines PECB Certified Human Ressources Decurity Foundation Jour 1 : Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2 : Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis : Aucun Certification : Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification			2	450 000
27035		Jour 1 : Introduction aux principes et concepts fondamentaux de la gestion des		
Jour 2 : Approches processus de gestion des incidents de la sécurité de l'information et examen de certification Prérequis : Aucun Certification :		incidents de la sécurité de l'information, tels que définis par la norme ISO/CEI		
l'information et examen de certification Prérequis : Aucun Certification : PECB Certified ISO/IEC 27035 Lead Incident Manager Jour 1 Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/CEI 27035 Jour 2 Conception et préparation d'un plan de gestion des incidents de sécurité de l'information Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 4 Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information Jour 5 Examen de certification 11 Formations en sécurité des ressources humaines PECB Certified Human Ressources Security Foundation Jour 1 : Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2 : Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis : Aucun Certification : Cybersécurité 1				
Prérequis : Aucun Certification : PECB Certified ISO/IEC 27035 Lead Incident Manager Jour 1 Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/CEI 27035 Jour 2 Conception et préparation d'un plan de gestion des incidents de sécurité de l'information Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 4 Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information Jour 5 Examen de certification 11 Formations en sécurité des ressources humaines PECB Certified Human Ressources Security Foundation Jour 1 : Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2 : Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis : Aucun Certification : Cybersécurité 1		Jour 2 : Approches processus de gestion des incidents de la sécurité de		
Certification: PECB Certified ISO/IEC 27035 Lead Incident Manager Jour 1 Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/CEI 27035 Jour 2 Conception et préparation d'un plan de gestion des incidents de sécurité de l'information Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 5 Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information Jour 5 Examen de certification 11 Pormations en sécurité des ressources humaines PECB Certified Human Ressources Security Foundation Jour 1 : Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2 : Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis : Aucun Certification : Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification		l'information et examen de certification		
PECB Certified ISO/IEC 27035 Lead Incident Manager Jour 1 Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/CEI 27035 5 950 000 Jour 2 Conception et préparation d'un plan de gestion des incidents de sécurité de l'information Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 4 Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information Jour 5 Examen de certification Formations en sécurité des ressources humaines PECB Certified Human Ressources Security Foundation Jour 1: Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2: Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis: Aucun Certification: Cybersécurité ISO/IEC 27032 Formation ISO/IEC 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification		<u>Prérequis</u> : Aucun		
Jour 1 Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/CEI 27035 Jour 2 Conception et préparation d'un plan de gestion des incidents de sécurité de l'information Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 4 Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information Jour 5 Examen de certification 11 Formations en sécurité des ressources humaines PECB Certified Human Ressources Security Foundation Jour 1 : Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2 : Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis : Aucun Certification : Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification		<u>Certification</u> :		
Jour 1 Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/CEI 27035 Jour 2 Conception et préparation d'un plan de gestion des incidents de sécurité de l'information Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 4 Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information Jour 5 Examen de certification 11 Formations en sécurité des ressources humaines PECB Certified Human Ressources Security Foundation Jour 1 : Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2 : Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis : Aucun Certification : Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification				
l'information, tels que définis par l'ISO/CEI 27035 Jour 2 Conception et préparation d'un plan de gestion des incidents de sécurité de l'information Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 4 Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information Jour 5 Examen de certification 11 Formations en sécurité des ressources humaines PECB Certified Human Ressources Security Foundation Jour 1 : Introduction aux concepts fondamentaux de la sécurité des ressources humaines et les qu'exigés par ISO/IEC 27001 Jour 2 : Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis : Aucun Certification : Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification		PECB Certified ISO/IEC 27035 Lead Incident Manager		
Jour 2 Conception et préparation d'un plan de gestion des incidents de sécurité de l'information Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 4 Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information Jour 5 Examen de certification 11 Formations en sécurité des ressources humaines PECB Certified Human Ressources Security Foundation Jour 1 Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2 Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis Aucun Certification Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification		: =		
de l'information Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 4 Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information Jour 5 Examen de certification 11 Formations en sécurité des ressources humaines PECB Certified Human Ressources Security Foundation Jour 1: Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2: Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis: Aucun Certification: Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification			5	950 000
Jour 3 Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information Jour 4 Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information Jour 5 Examen de certification				
incidents de sécurité de l'information Jour 4 Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information Jour 5 Examen de certification 11 Formations en sécurité des ressources humaines PECB Certified Human Ressources Security Foundation Jour 1: Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2: Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis: Aucun Certification: Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification				
Jour 4 Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information Jour 5 Examen de certification				
sécurité de l'information Jour 5 Examen de certification 11 Formations en sécurité des ressources humaines PECB Certified Human Ressources Security Foundation Jour 1: Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2: Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis: Aucun Certification: Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification				
Jour 5 Examen de certification		. · · · · ·		
11 Formations en sécurité des ressources humaines PECB Certified Human Ressources Security Foundation Jour 1: Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2: Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis: Aucun Certification: Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification				
PECB Certified Human Ressources Security Foundation Jour 1: Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2: Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis: Aucun Certification: Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification		<u>Jour 5</u> Examen de certification		
PECB Certified Human Ressources Security Foundation Jour 1: Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2: Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis: Aucun Certification: Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification	11	Formations en sécurité des ressources humaines		
Jour 1 : Introduction aux concepts fondamentaux de la sécurité des ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2 : Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis : Aucun Certification : Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification	11			
ressources humaines tels qu'exigés par ISO/IEC 27001 Jour 2 : Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis : Aucun Certification: Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification				
Jour 2 : Sensibilisation, éducation et formation, actions disciplinaires, changement des responsabilités liées au contrat de travail Prérequis : Aucun Certification :				
changement des responsabilités liées au contrat de travail Prérequis: Aucun Certification: Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification				
Prérequis : Aucun Certification : Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification				
Cybersécurité 1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification				
1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification				
1 ISO/IEC 27032 Formation ISO/CEI 27032 Lead Cybersecurity Manager Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification		Cybersécurité		
Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification	1	<u> </u>	5	950 000
recommandation de la norme ISO/IEC 27032 Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification				
Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification				
d'attaque Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification				
Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification				
l'information Jour 4 Gestion des incidents, suivi et amélioration continue Jour 5 Examen de certification		•		
Jour 5 Examen de certification				
Jour 5 Examen de certification		Jour 4 Gestion des incidents, suivi et amélioration continue		
2 Cloud Security				
2 Cloud Security				
2 Cloud Security				
	2	Cloud Security		

Jour 1 Introduction aux normes ISO/IEC 27017 et ISO/IEC 27018 et à l'initiation d'un programme de sécurité du cloud Jour 2 Gestion des risques de sécurité du cloud computing et mesures spécifiques au cloud Jour 3 Gestion de l'information documentée et sensibilisation et formation à la sécurité du cloud Jour 4 Gestion des incidents de sécurité du cloud, tests, surveillance et amélioration continue Jour 5 Examen de certification Formation professionnelle - Tests d'intrusion PECB Certified Lead Pen Test Professional Jour 1 Introduction aux tests d'intrusions, à l'éthique, à la planification et au domaine d'application Jour 2 Connaissances techniques fondamentales et techniques (avec des exercices pratiques dans tous les domaines) Jour 3 Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test Jour 4 Analyse des résultats des tests, rapports et suivi Jour 5 Examen de certification 4			
d'un programme de sécurité du cloud Jour 2 Gestion des risques de sécurité du cloud computing et mesures spécifiques au cloud Jour 3 Gestion de l'information documentée et sensibilisation et formation à la sécurité du cloud Jour 4 Gestion des incidents de sécurité du cloud, tests, surveillance et amélioration continue Jour 5 Examen de certification Jour 5 Examen de certification Formation professionnelle - Tests d'intrusion PECB Certified Lead Pen Test Professional Jour 1 Introduction aux tests d'intrusions, à l'éthique, à la planification et au domaine d'application Jour 2 Connaissances techniques fondamentales et techniques (avec des exercices pratiques dans tous les domaines) Jour 3 Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test Jour 4 Analyse des résultats des tests, rapports et suivi Jour 5 Examen de certification Piratage éthique — Formations et certifications PECB Certified Lead Ethical Hacker Day 1 Introduction to ethical hacking Day 2 Initiating the reconnaissance phase Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam PECB Certified Computer Forensics Foundation Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Prérequis : Aucun Certification : Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques	950 000	5	Certified Lead Cloud Security Manager
Jour 2 Gestion des risques de sécurité du cloud computing et mesures spécifiques au cloud Jour 3 Gestion de l'information documentée et sensibilisation et formation à la sécurité du cloud Jour 4 Gestion des incidents de sécurité du cloud, tests, surveillance et amélioration continue Jour 5 Examen de certification 3 Formation professionnelle - Tests d'intrusion PECB Certified Lead Pen Test Professional Jour 1 Introduction aux tests d'intrusions, à l'éthique, à la planification et au domaine d'application Jour 2 Connaissances techniques fondamentales et techniques (avec des exercices pratiques dans tous les domaines) Jour 3 Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test Jour 4 Analyse des résultats des tests, rapports et suivi Jour 5 Examen de certification 4 Piratage éthique — Formations et certifications PECB Certified Lead Ethical Hacker Day 1 Introduction to ethical hacking Day 2 Initiating the reconnaissance phase Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam PecB Certified Computer Forensics Foundation Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Préreguis : Aucun Certification : Après avoir réussi l'examen, les participants peuvent demander la qualification s PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics Foundation informatique Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques Jour 3 Analyse et gestion des			
au cloud Jour 3 Gestion de l'information documentée et sensibilisation et formation à la sécurité du cloud Jour 4 Gestion des incidents de sécurité du cloud, tests, surveillance et amélioration continue Jour 5 Examen de certification 3 Formation professionnelle - Tests d'intrusion PECB Certified Lead Pen Test Professional Jour 1 Introduction aux tests d'intrusions, à l'éthique, à la planification et au domaine d'application Jour 2 Connaissances techniques fondamentales et techniques (avec des exercices pratiques dans tous les domaines) Jour 3 Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test Jour 4 Analyse des résultats des tests, rapports et suivi Jour 5 Examen de certification 4 Piratage éthique — Formations et certifications PECB Certified Lead Ethical Hacker Day 1 Introduction to ethical hacking Day 2 Initiating the reconnaissance phase Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam 5 Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Prérequis : Aucun Certification : Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			
Jour 3 Gestion de l'information documentée et sensibilisation et formation à la sécurité du cloud Jour 4 Gestion des incidents de sécurité du cloud, tests, surveillance et amélioration continue Jour 5 Examen de certification 5			<u>Jour 2</u> Gestion des risques de sécurité du cloud computing et mesures spécifiques
Sécurité du cloud Jour 4 Gestion des incidents de sécurité du cloud, tests, surveillance et amélioration continue Jour 5 Examen de certification			au cloud
Jour 4 Gestion des incidents de sécurité du cloud, tests, surveillance et amélioration continue Jour 5 Examen de certification			Jour 3 Gestion de l'information documentée et sensibilisation et formation à la
amélioration continue Jour 5 Examen de certification Formation professionnelle - Tests d'intrusion PECB Certified Lead Pen Test Professional Jour 1 Introduction aux tests d'intrusions, à l'éthique, à la planification et au domaine d'application Jour 2 Connaissances techniques fondamentales et techniques (avec des exercices pratiques dans tous les domaines) Jour 3 Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test Jour 4 Analyse des résultats des tests, rapports et suivi Jour 5 Examen de certification 4 Piratage éthique — Formations et certifications PECB Certified Lead Ethical Hacker Day 1 Introduction to ethical hacking Day 2 Initiating the reconnaissance phase Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam 5 Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Prérequis : Aucun Certification : Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			sécurité du cloud
amélioration continue Jour 5 Examen de certification Formation professionnelle - Tests d'intrusion PECB Certified Lead Pen Test Professional Jour 1 Introduction aux tests d'intrusions, à l'éthique, à la planification et au domaine d'application Jour 2 Connaissances techniques fondamentales et techniques (avec des exercices pratiques dans tous les domaines) Jour 3 Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test Jour 4 Analyse des résultats des tests, rapports et suivi Jour 5 Examen de certification 4 Piratage éthique — Formations et certifications PECB Certified Lead Ethical Hacker Day 1 Introduction to ethical hacking Day 2 Initiating the reconnaissance phase Day 3 Initiating the reconnaissance phase Day 4 Post-exploitation and reporting Day 5 Certification exam 5 Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Prérequis : Aucun Certification : Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			Jour 4 Gestion des incidents de sécurité du cloud, tests, surveillance et
Jour 5 Examen de certification Formation professionnelle - Tests d'intrusion PECB Certified Lead Pen Test Professional Jour 1 Introduction aux tests d'intrusions, à l'éthique, à la planification et au domaine d'application Jour 2 Connaissances techniques fondamentales et techniques (avec des exercices pratiques dans tous les domaines) Jour 3 Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test Jour 4 Analyse des résultats des tests, rapports et suivi Jour 5 Examen de certification 4 Piratage éthique — Formations et certifications PECB Certified Lead Ethical Hacker Day 1 Introduction to ethical hacking Day 2 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam 5 Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1: Introduction aux processus d'investigation judiciaire Jour 2: processus d'investigation judiciaire et examen de certification Prérequis: Aucur Certification: Après avoir réussi l'examen, les participants peuvent demander la qualification ex PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques Jour 3 Analyse et gestion des artefacts			
Formation professionnelle - Tests d'intrusion PECB Certified Lead Pen Test Professional Jour 1 Introduction aux tests d'intrusions, à l'éthique, à la planification et au domaine d'application Jour 2 Connaissances techniques fondamentales et techniques (avec des exercices pratiques dans tous les domaines) Jour 3 Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test Jour 4 Analyse des résultats des tests, rapports et suivi Jour 5 Examen de certification 4 Piratage éthique — Formations et certifications PECB Certified Lead Ethical Hacker Day 1 Introduction to ethical hacking Day 2 Initiating the exploitation phase Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam 5 Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Prérequis : Aucun Certification: Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			
PECB Certified Lead Pen Test Professional Jour 1 Introduction aux tests d'intrusions, à l'éthique, à la planification et au domaine d'application Jour 2 Connaissances techniques fondamentales et techniques (avec des exercices pratiques dans tous les domaines) Jour 3 Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test Jour 4 Analyse des résultats des tests, rapports et suivi Jour 5 Examen de certification 4 Piratage éthique — Formations et certifications PECB Certified Lead Ethical Hacker Day 1 Introduction to ethical hacking Day 2 Initiating the reconnaissance phase Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam 5 Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Prérequis : Aucun Certification : Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			<u>Jour 5</u> Examen de certification
PECB Certified Lead Pen Test Professional Jour 1 Introduction aux tests d'intrusions, à l'éthique, à la planification et au domaine d'application Jour 2 Connaissances techniques fondamentales et techniques (avec des exercices pratiques dans tous les domaines) Jour 3 Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test Jour 4 Analyse des résultats des tests, rapports et suivi Jour 5 Examen de certification 4			Formation professionnelle - Tests d'intrusion
Jour 1 Introduction aux tests d'intrusions, à l'éthique, à la planification et au domaine d'application Jour 2 Connaissances techniques fondamentales et techniques (avec des exercices pratiques dans tous les domaines) Jour 3 Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test Jour 4 Analyse des résultats des tests, rapports et suivi Jour 5 Examen de certification 4 Piratage éthique — Formations et certifications PECB Certified Lead Ethical Hacker Day 1 Introduction to ethical hacking Day 2 Initiating the reconnaissance phase Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam Formations en investigation légale informatique 5 Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Préreguis : Aucun Certification : Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques	950 000	5	
domaine d'application Jour 2 Connaissances techniques fondamentales et techniques (avec des exercices pratiques dans tous les domaines) Jour 3 Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test Jour 4 Analyse des résultats des tests, rapports et suivi Jour 5 Examen de certification 4 Piratage éthique — Formations et certifications PECB Certified Lead Ethical Hacker Day 1 Introduction to ethical hacking Day 2 Initiating the reconnaissance phase Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam 5 Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1: Introduction aux processus d'investigation judiciaire Jour 2: processus d'investigation judiciaire et examen de certification Préreguis: Aucun Certification: Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			·
Jour 2 Connaissances techniques fondamentales et techniques (avec des exercices pratiques dans tous les domaines) Jour 3 Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test Jour 4 Analyse des résultats des tests, rapports et suivi Jour 5 Examen de certification 4 Piratage éthique — Formations et certifications PECB Certified Lead Ethical Hacker			
exercices pratiques dans tous les domaines) Jour 3 Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test Jour 4 Analyse des résultats des tests, rapports et suivi Jour 5 Examen de certification 4 Piratage éthique — Formations et certifications PECB Certified Lead Ethical Hacker Day 1 Introduction to ethical hacking Day 2 Initiating the reconnaissance phase Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam 5 Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Préreguis : Aucun Certification: Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			
Jour 3 Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test Jour 4 Analyse des résultats des tests, rapports et suivi Jour 5 Examen de certification 4 Piratage éthique — Formations et certifications PECB Certified Lead Ethical Hacker 5 Day 1 Introduction to ethical hacking Day 2 Initiating the reconnaissance phase Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam Formations en investigation légale informatique 5 Formations en investigation légale informatique 2 PECB Certified Computer Forensics Foundation 2 Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Prérequis : Aucun Certification : Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			· · · · · · · · · · · · · · · · · · ·
du domaine du test Jour 4 Analyse des résultats des tests, rapports et suivi Jour 5 Examen de certification 4 Piratage éthique — Formations et certifications PECB Certified Lead Ethical Hacker Day 1 Introduction to ethical hacking Day 2 Initiating the reconnaissance phase Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam 5 Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Prérequis : Aucun Certification : Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			
Jour 4 Analyse des résultats des tests, rapports et suivi Jour 5 Examen de certification 4 Piratage éthique — Formations et certifications PECB Certified Lead Ethical Hacker Day 1 Introduction to ethical hacking Day 2 Initiating the reconnaissance phase Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam 5 Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Prérequis : Aucun Certification : Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			
Jour 5 Examen de certification Piratage éthique — Formations et certifications PECB Certified Lead Ethical Hacker Day 1 Introduction to ethical hacking Day 2 Initiating the reconnaissance phase Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam Formations en investigation légale informatique			
4 Piratage éthique — Formations et certifications PECB Certified Lead Ethical Hacker Day 1 Introduction to ethical hacking Day 2 Initiating the reconnaissance phase Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam 5 Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1: Introduction aux processus d'investigation judiciaire Jour 2: processus d'investigation judiciaire et examen de certification Prérequis: Aucun Certification: Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			
PECB Certified Lead Ethical Hacker Day 1 Introduction to ethical hacking Day 2 Initiating the reconnaissance phase Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam 5 Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Prérequis : Aucun Certification : Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			<u>Jour 5</u> Examen de certification
PECB Certified Lead Ethical Hacker Day 1 Introduction to ethical hacking Day 2 Initiating the reconnaissance phase Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam 5 Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Prérequis : Aucun Certification : Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			Directors (this was Formactions at contifications
Day 1 Introduction to ethical hacking Day 2 Initiating the reconnaissance phase Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam 5 Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Prérequis : Aucun Certification : Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques	050.000	_	
Day 2 Initiating the reconnaissance phase Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam 5 Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1: Introduction aux processus d'investigation judiciaire Jour 2: processus d'investigation judiciaire et examen de certification Prérequis: Aucun Certification: Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques	950 000	5	
Day 3 Initiating the exploitation phase Day 4 Post-exploitation and reporting Day 5 Certification exam 5 Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1: Introduction aux processus d'investigation judiciaire Jour 2: processus d'investigation judiciaire et examen de certification Prérequis: Aucun Certification: Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			
Day 4 Post-exploitation and reporting Day 5 Certification exam Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Prérequis : Aucun Certification : Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			
Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Prérequis : Aucun Certification : Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			
Formations en investigation légale informatique PECB Certified Computer Forensics Foundation Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Prérequis : Aucun Certification : Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			
PECB Certified Computer Forensics Foundation Jour 1: Introduction aux processus d'investigation judiciaire Jour 2: processus d'investigation judiciaire et examen de certification Prérequis: Aucun Certification: Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			<u>Day 5</u> Certification exam
Jour 1: Introduction aux processus d'investigation judiciaire Jour 2: processus d'investigation judiciaire et examen de certification Prérequis: Aucun Certification: Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			Formations en investigation légale informatique
Jour 1 : Introduction aux processus d'investigation judiciaire Jour 2 : processus d'investigation judiciaire et examen de certification Prérequis : Aucun Certification : Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques	450 000	2	DECD Contified Commuter Forencies Foundation
Jour 2 : processus d'investigation judiciaire et examen de certification Prérequis : Aucun Certification : Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques	450 000	2	
Prérequis: Aucun Certification: Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			· · · · · · · · · · · · · · · · · · ·
Certification: Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			
la qualification « PECB Certified Computer Forensics Foundation ». Pour plus d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			
d'informations concernant les certifications Computer Forensics et le processus de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			<u>Certification</u> : Après avoir réussi l'examen, les participants peuvent demander
de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			la qualification « PECB Certified Computer Forensics Foundation ». Pour plus
de certification PECB. PECB Certified Lead Computer Forensics Examiner Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			d'informations concernant les certifications Computer Forensics et le processus
Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			
Jour 1 Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			
informatique Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques	950 000	5	
Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			<u>Jour 1</u> Introduction à la réponse aux incidents et concepts relatifs à l'investigation
Jour 2 Préparer et diriger une enquête informatique judiciaire Jour 3 Analyse et gestion des artefacts numériques			informatique
Jour 3 Analyse et gestion des artefacts numériques			·
LIOUE + FICSEIHAUOH UU CAS ELIEUX DE SIDUMATION			Jour 4 Présentation du cas et jeux de simulation
Jour 5 Examen de certification			· · · · · · · · · · · · · · · · · · ·
6 Cybersecurity Maturity Model Certification			
	450 000	2	
avec les concepts de base et les exigences du modèle CMMC)	.50 500	_	
Jour 1: Introduction à l'écosystème CMMC et au modèle CMMC			=
Jour 2 : Pratiques CMMC, processus d'évaluation et code de déontologie			
Prérequis : Aucun			
<u>Certification</u> : Après avoir réussi l'examen, vous pouvez demander la certification			
mentionnée dans le tableau ci-dessous. Pour plus d'informations sur le processus			·
	1		
de certification de PECB			de certification de PECB

	CMMC Certified Professional	4	850 000
	Jour 1 Introduction aux parties prenantes, au modèle et aux pratiques CMMC de	7	030 000
	niveau 1		
	Jour 2 Processus et pratiques CMMC des niveaux 2 et 3		
	Jour 3 Processus et pratiques CMMC des niveaux 4 et 5		
	Jour 4 Rôles et responsabilités, éthique et méthodologie d'évaluation de		
	l'écosystème CMMC-AB		
	Continuité, Résilience et Reprise		
1	Formations ISO 22301 Systèmes de management de la continuité d'activité		
	ISO 22301 Introduction	1	220 000
	Jour 1 : Introduction aux concepts du Système de management de la continuité		
	d'activité, tels que définis par la norme ISO 22301		
	<u>Prérequis</u> : aucun		
	PECB Certified ISO 22301 Foundation	2	450 000
	Jour 1 : Introduction au système de management de la continuité d'activité	_	.55 555
	(SMCA) et à ISO 22301		
	Jour 2 : Système de management de la continuité d'activité et examen de		
	certification		
	<u>Prérequis</u> : aucun		
	<u>Certification</u> : Après avoir réussi l'examen, les participants peuvent demander la		
	qualification « PECB Certified ISO 22301 Foundation ». Pour plus d'informations		
	concernant les certifications ISO 22301 et le processus de certification PECB.		
	PECB Certified ISO 22301 Lead Auditor		
	Jour 1 Introduction au système de management de la continuité d'activité (SMCA)		
	et à ISO 22301	5	950 000
	Jour 2 Principes d'audit, préparation et déclenchement d'un audit		
	Jour 3 Activités d'audit sur site		
	<u>Jour 4</u> Clôture de l'audit		
	<u>Jour 5</u> Examen de certification		
	Gouvernance, Risque et conformité		
	ISO 31000 Management du risque		
	ISO 31000 Introduction (Introduction au management du risque, conforme à la	1	
	norme ISO 31000)	_	
	Jour 1 : Introduction au management du risque selon les principes et les lignes		
	directrices de la norme ISO 31000		
	<u>Prérequis</u> : aucun		
	PECB Certified ISO 31000 Foundation	2	
	<u>Jour 1</u> : Introduction aux concepts de management du risque, tels que définis par la norme ISO 31000		
	Jour 2 : Processus de management du risque et examen de certification		
	Prérequis : aucun		
	<u>Certification</u> : Après avoir réussi l'examen, les participants peuvent demander la		
	qualification « PECB Certified ISO 31000 Foundation ». Pour plus d'informations		
	concernant les certifications ISO 31000 et le processus de certification PECB		
	PECB Certified ISO 31000 Lead Risk Manager		
	Jour 1 Introduction à la norme ISO 31000 et aux processus de management du		
	risque	5	
	Jour 2 Établissement du contexte, appréciation et traitement du risque selon la	-	
	norme ISO 31000		

<u>Jour 3</u> Acceptation, communication et concertation, enregistrement et rapports,	
surveillance et revue du risque selon la norme ISO 31000	
Jour 4 Techniques d'appréciation du risque conformes à la norme CEI/ISO 31010	
Jour 5 Examen de certification	
Protection de la Vie Privée et des Données	
<u>Transformation numérique</u>	
Qualité et Management	
<u>Durabilité</u>	