





# M1 CPIR spécialisation SiiC

## modules Sécurité du Cloud

- 1- Le Cloud = 14h.
- 2- Développement Cloud = 14h.
- 3- Admin Cloud = 14h.

# whoami

Guillaume Moulard

Oracle

- consulting et avant vente BD et internet

Orange

- Projet BOND - Création internet avec intégration de 52 serveurs
- Mail Orange 40 +4 Millions BAL sur des milliers de machines
- Architect projet cloud sur Openwatt, Cloudwatt et flexible engine

# Les Blocs

Bloc	Bloc de compétence	Compétence	Description	Modalités	Modules de formation	Durée (h)
Sécurité informatique des infrastructures systèmes et réseaux	Connaître les menaces	Connaître les types de menaces et de solutions	ARP Cache Poisoning, ARP/DHCP Spoofing, HSRP/VRRP spoofing, STP/VTP Attacks, DMZ, NAT, Redirection de flux, détection d'intrusions,		Hacher éthique	14
	Connaître les réseaux IP	Architectures et protocoles des réseaux ip	Routage avancé, Qualité de service, Protocoles de signalisation, QoS, Vlan, ....		Réseaux IP et qualité de service	14
	Sécurité des accès et des échanges	Assurer la sécurité des échanges	Chiffrement, codages, protocoles, SSL, SSL/TLS, IPSEC, L2TP, etc., architectures		Sécurité des échanges	14
		Assurer la sécurité des accès	Sécurité périmétrique, services d'annuaires, admin windows et unix, filtrage d'accès, Firewall, proxys, IMS....		Sécurité des accès	14
	Sécurité systèmes et des applications	Sécuriser les systèmes d'exploitation et les services applicatifs	Appels systèmes, programmation et sécurité		Sécurité des systèmes et applis	14
	Supervision système et réseau	Superviser les infrastructures	Administration des systèmes, exploitation, maintenance et supervision des infrastructures		Supervision des infrastructures	14
	Total					84



# Les Blocs

Bloc	Bloc de compétence	Compétence	Description	Modalités	Modules de formation	Durée (h)
Sécurité des mobiles, du Cloud et de l'IoT	Sécuriser les mobiles	Réseaux sans fil et mobiles	Normes, Wi-Fi, UMTS, GPRS, LTE		Réseaux sans fil	14
		Sécuriser les mobiles	Accès mobiles, convergence fixe-mobile, sécurité des mobiles		Sécurité des mobiles	14
	Sécuriser les Objets Connectés	Connaitre les objets connectés, les protocoles, ...	Réseaux de l'IoT (Sigfox, LoRa, réseaux de terrain, SCADA,...)		Internet des objets connectés (IoT)	14
		Connaitre les failles de sécurité de l'IoT	Sécurité des systèmes embarqués, attaques internet, attaques Stunex, hackaton ?		Sécurité de l'IoT	14
	Sécuriser le Cloud	Savoir choisir une solution de Cloud	xAAS, Types et architectures du cloud, Acteurs du cloud		Le Cloud	14
		Savoir virtualiser un système, un stockage, un réseau	Outils, Virtualisation de serveurs Vmware, SDI, SDN, NFV		Virtualisation	8
		Savoir développer en Cloud	Développer une appli avec AWS		Développement Cloud	14
		Savoir administrer un Cloud	Admin d'Open stack ou d'Azure		Admin Cloud	14
	Sécuriser par conception	Maitriser la sécurité par design	Maitriser la sécurité dès l'étape de conception d'un système		Securité par conception	7
	Total					113

# Les Blocs

Bloc	Bloc de compétence	Compétence	Description	Modalités	Modules de formation	Durée (h)
Sécurité des données	Données et Web	Contrôler les comportements aberrants des collaborateurs	Système de détection des comportements anormaux		Outils d'analyse comportementale à base d'IA	7
		Sécuriser les SGBD et les entrepôts de données	SGBD et gestion avancés des droits, journalisation, sauvegardes et restitution, données sensibles		Administration de SGBD, OLAP, ...	14
		Connaître les technologies du web et leurs points faibles	Langages et environnements Web		Sécurité du Web	14
		Connaître les outils du Big Data et leurs failles potentielles	Données semi-structures et non structurées, extraction de connaissances, RI, profil et communautés d'utilisateurs		Big data et aide à la décision	7
	Total					42
Gestion de projet et culture ingénieur	Connaître les méthodes de la sûreté de fonctionnement	Connaître les méthodes de test et de validation	Méthodes et outils de test, de validation, de preuve formelle		Test et validation	7
	Méthodes de la sécurité informatique	Connaître les méthodes et techniques de la sécurité informatique, savoir piloter	Gestion des risques, Cyber-Diagnostic, PSSI, social engineering, EBIOS, MEHARI, etc...		Méthodologie de la SIIC	16
		Connaître les normes et standards de l'assurance contre les risques	Common criteria(ISO/IEC 15408), acteurs (autorité de confiance (ex ANSSI), évaluateurs, développeur)		Normes et standards de la Sécurité	7
	Business	Savoir élaborer un cahier des charges et répondre à un appel	Compléter el chapitre sécuritaire d'un AO. Analyser la répondre au chapitre sécuritaire		CC et AO	7
	Loi et éthique	Loi et données informatiques, morale et éthique	CNIL, notions de droit commercial et international		Loi et éthique	4
	Total					41

# M1-CPIR-Siic : Cloud

**Objectifs**

- Comprendre implication des offres 'as a Service'.
- Identifier les segmentations habituelles des offres XaaS.
- Comprendre les usages Types d'infrastructure cloud : public, privé, hybride,VPC.
- Comparé les solutions d'architectures du cloud : Openstack, AWS, salesforce
- Connaitre et savoir identifier les acteurs du cloud

Type Cours /TD/TP ...	Titre	Durée (h)	Descriptif
C	De l'ordinateur au Cloud	4	Présentation du process de mise en place d'application dans des infrastructures physiques, son pendant pour les déploiements dans le cloud. Préparation des exposés fait par les étudiants
C	Cloud typologie	4	Présentation des différentes typologies de cloud XaaS / Cloud privé, public, hybride. Présentation par les étudiants des Offres AWS, Asure, OVH, Salesforce
C	Détail Openstack	4	Présentation technique Openstack Démonstration par les étudiants : Création VM, Network, Security group, stack



# M1-CPIR-SiiC : devCloud

Objectifs

- Découverte des modèles et outils devops
- Identification des impacts du cloud dans la conception logiciels
- Prise en compte des problématiques sécurité et vendor locking des outils du cloud.

	Titre	Durée (h)	Descriptif
C	conception logiciel	4	Présentation de paterne d'application cloud ready Les processus de scalabilité et les stratégies micro service création d'environnement applicatif chez AWS
C	déploiement d'application	4	création d'une application type DB / WAS / WEB mise en œuvre de d'une gestion de version applicative. présentation par les étudiants : chaos monkey, Route 53, Ancible, la haute disponibilité.
C	Sécurisation	4	Problématique de sécurisation des données Gestion des accées aux infrastructures Application multi-cloud Présentation par les étudiants : Gestion de clef SSH, outil d'anonymisation de données, N7, Cassandra



# M1-CPIR-SiiC : Administration Cloud

Objectifs

- Connaître Openstack, sa fondation, ses composants sont organisation interne
- Installer une distribution Openstack
- Créer des projets des utilisateurs et des ressources.

C	Présentation Openstack	4	Présentation détaillée d'Openstack : <ul style="list-style-type: none"><li>- organisation de la fondation</li><li>- présentation des versions et des distro</li><li>- Les modules d'Openstack leurs interactions et leurs API</li></ul> Utilisation de trystack
C	Installation Openstack	4	installation dans une VM d'une version d'openstack all on one
C	Administration Openstack	4	Finalisation de l'installation ajout de ressource au cloud setup de user / et de projets
Exam.		2	

# TP – PI / VM

- 3 Groupes / 3 questions
- Quels sont les avantages du Raspberry PI ?
  - IOT, Consommation électrique, taille, prix, CAPEX-Achat
- Quels sont les avantages d'une VM sur un serveur ?
  - Deployment, puissance, dispo, modularité, backup, CAPEX-Achat
- Quels sont les avantages d'une VM dans le cloud ?
  - pas de maintenance physique/DC, dispo, pas d'obsolescence physique, backup, SLA, OPEX-Location

CAPEX : Capital Expenditure, OPEX : Operation

# Pourquoi les entreprises aiment le cloud

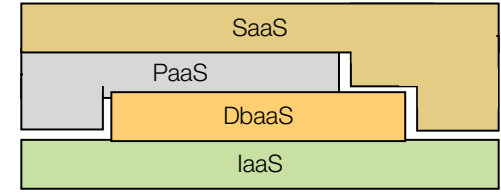
- Flexibilité
- Financier
  - pas CAPEX
  - évolution des OPEX lineaire par rapport aux besoins
- matériel
  - Disponibilité de l'infrastructure
    - Si plusieurs site
  - Encombrement dans les locaux de l'entreprise
  - Pas de gestion du Datacenter
- SLA
  - Engagement du prestataires

## 2. Le Cloud et Openstack ?

# Le cloud

- Le Cloud, ce sont des ressources informatiques externalisées, mise à disposition rapidement, facilement et en quantités (potentiellement) infinies
- Le Cloud, c'est une évolution technique, pas une révolution
  - Banalisation de l'utilisation de la virtualisation sur tous types de machines
  - Généralisation des solutions WebServices qui permettent les appels d'API vers des systèmes tiers
- Mais, c'est une révolution d'usage
  - Plus besoin de planifier de manière ferme les capacités nécessaires d'un point de vue infrastructure
  - Mais en contre partie, apparition d'un nouveau besoin : estimer plus finement la consommation effective à venir pour avoir une idée du budget
  - Les projets peuvent devenir maîtres de leur infrastructure, en la « créant » eux-mêmes, en fonction de leurs besoins

# La terminologie du Cloud

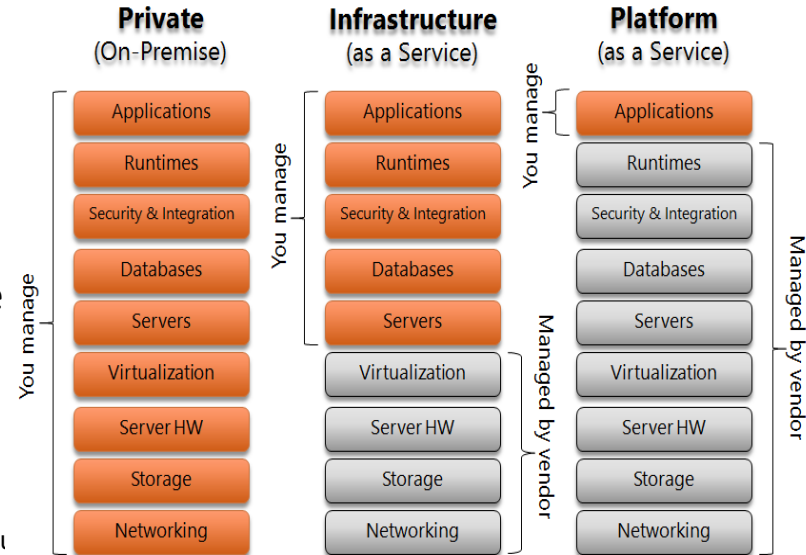


## ■ Les couches

- **IaaS** : Infrastructure matérielle louée à la demande
- **PaaS** : Plateforme logicielle louée à la demande
- **SaaS** : Solution logicielle clé en main, utilisable soit via le web soit par API

## ■ Des exemples

- chez nos concurrents:
  - IaaS: Amazon (public only) et Rackspace (public / privé) – client (netFix, airBnB, ...)
  - PaaS: Openshift de Redhat, AppEngine de Google
  - SaaS: Salesforce (CRM), Messagerie





# Magic Quadrant for Cloud Infrastructure as a Service, Worldwide

<https://www.gartner.com/doc/reprints?id=1-2G2O5FC&ct=150519>



# Magic Quadrant for Enterprise Application Platform as a Service, Worldwide (24 March 2016)

<https://www.gartner.com/technology/media-products/reprints/cybozu/277028.html?submissionGuid=607cc1a6-8d77-4532-9b4d-43fcb322a849>



# TP création VM Centos

- Sur les PC de l'école : Création avec Virtual BOX d'une VM.
- Quels sont les type d'images et les différences ?
  - iso, tgz, rpm
  - qcow2, vdi, vmdk, ova, qemu,
  - pct, lxc

Usage, Création, Modification





Et maintenant c'est **CAVOK** ?