Atelier n°1 : La sécurité dans les architectures cloud

LES JOURNÉES DE LA CYBER

2 & 3 MARS 2023
Campus Région du Numérique

LES JOURNÉES DE LA CYBER

Atelier n°1 : La sécurité dans les architectures cloud

Ludovic Coudrin
Cyber Security Sales Specialist
CISCO

Romain Touret
Cyber Security Sales Specialist
CISCO

Eddy Caron
ENS de Lyon - Chercheur
Co-fondateur de QIRINUS

Arthur Chevalier
Inria – Ingénieur transfert

CTO QIRINUS

LES JOURNÉES DE LA CYBER

CISCO, leader reconnu du Cloud

Cloud Networking

10M+

Appareils gérés dans le Cloud Meraki

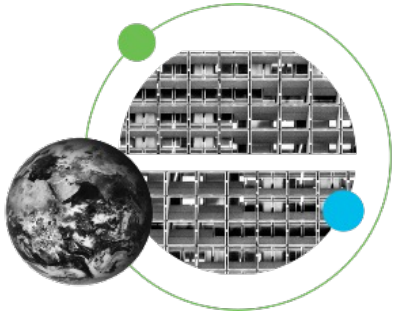
150M+

Appels API par mois sur le Cloud Meraki

Cloud Security

600Mds

Requêtes DNS par jour



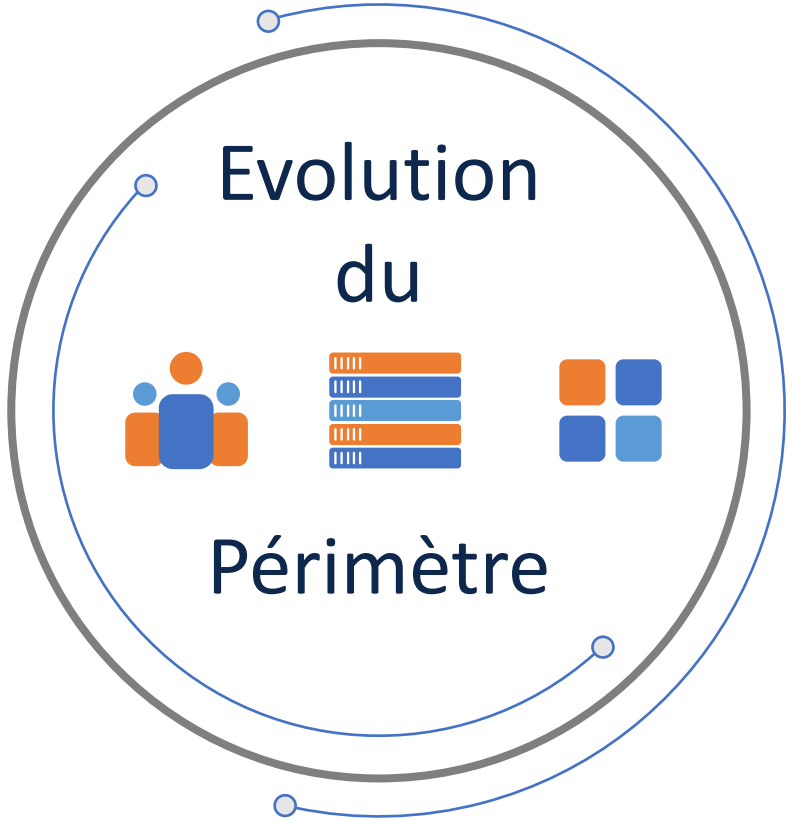
TALOS

Plus grand organisme mondial, non gouvernemental, de recheche contre les cyber-menaces

LES JOURNÉES DE LA CYBER

L'écosystème IT évolue

Les utilisateurs, les équipements et les applications sont partout



Utilisateurs distants

BYOD

IoT

Applications Cloud

Infrastructures hybrides

Infrastructures Cloud

LES JOURNÉES DE LA CYBER

Les risques IT évoluent

Le cybercriminalité explose et se professionnalise

RaaS

LockBit, Conti, ALPHV (BlackCat) avec des groupes associant ou partageant des membres (groupes DarkSide et Blackmatter)

+ 255% attaques par ransomware en 2022

Phishing

La pandémie de Covid a exacerbé les menaces de cyberattaques et les risques pesant sur les entreprises. 47% des télétravailleurs se sont fait piéger par un phishing en 2022.

Importance de la sensibilisation

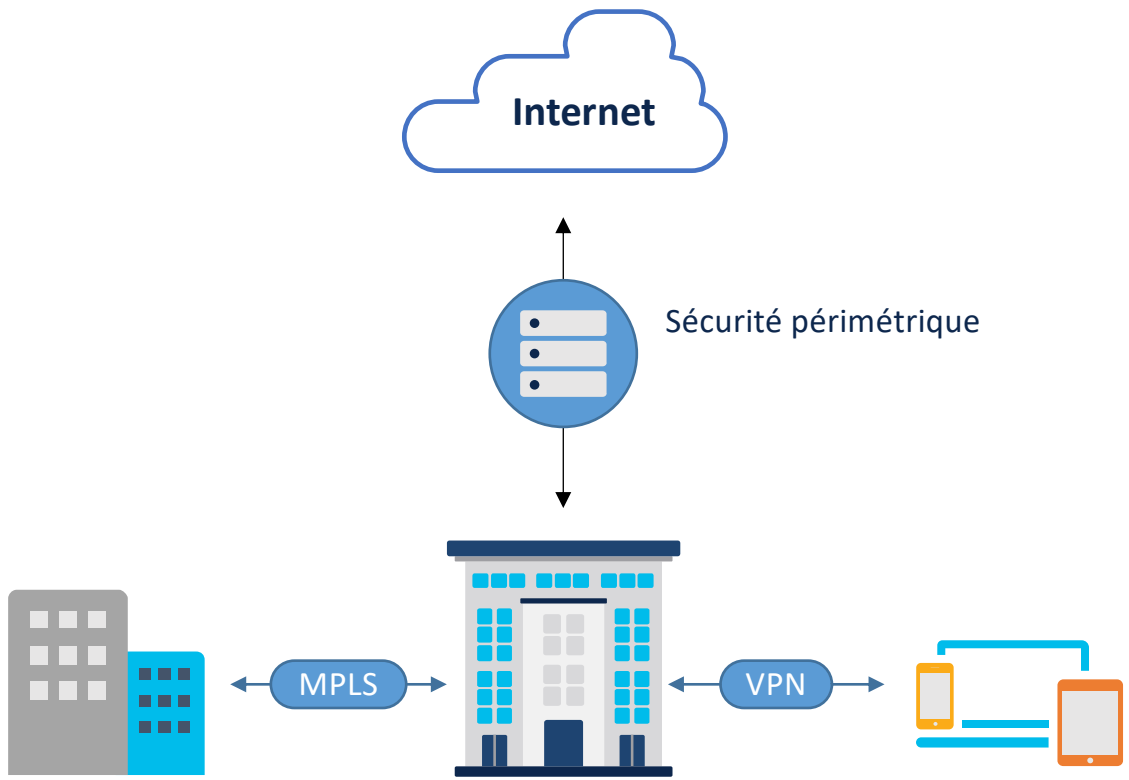
Extorsion

Chiffrement des fichiers, menace de divulgation des fichiers, name and shame, DDoS et RDoS pour pousser au paiement de la rançon.

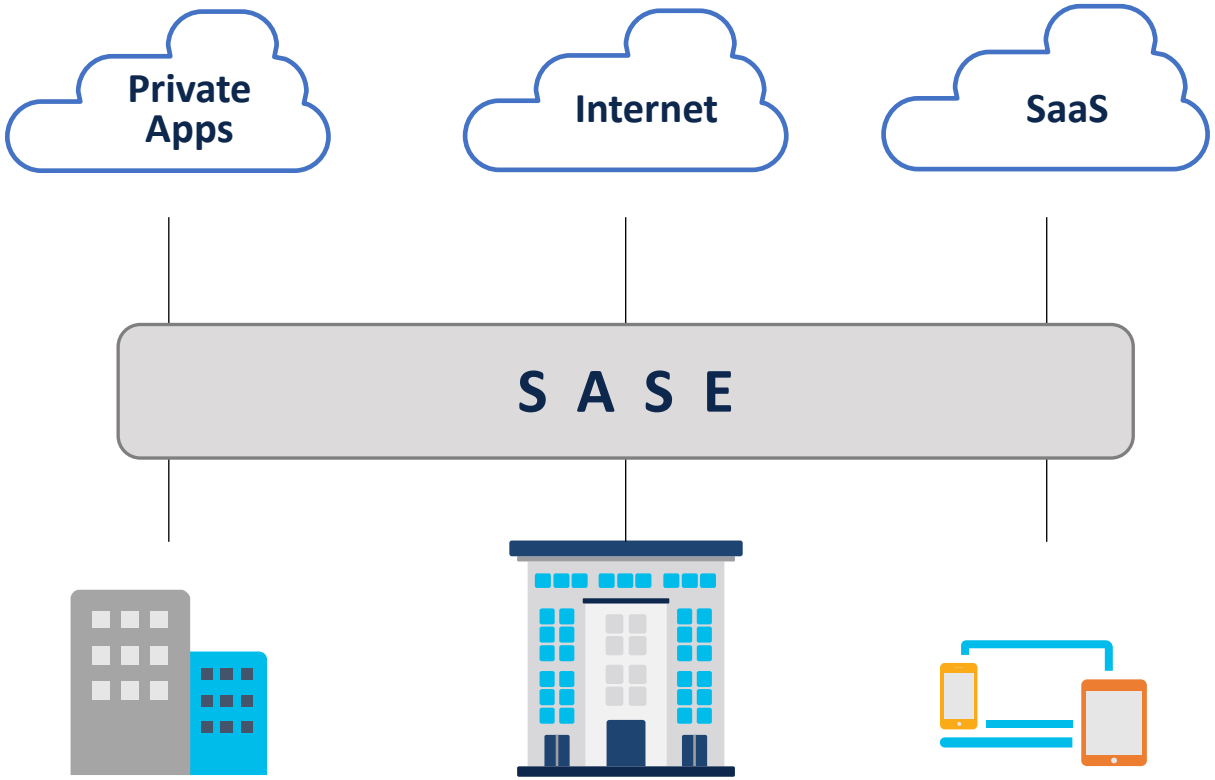
Les criminels font preuve de créativité

Sécuriser les infrastuctures et les accès

Un changement fondamental d'architecture



Approche centralisée



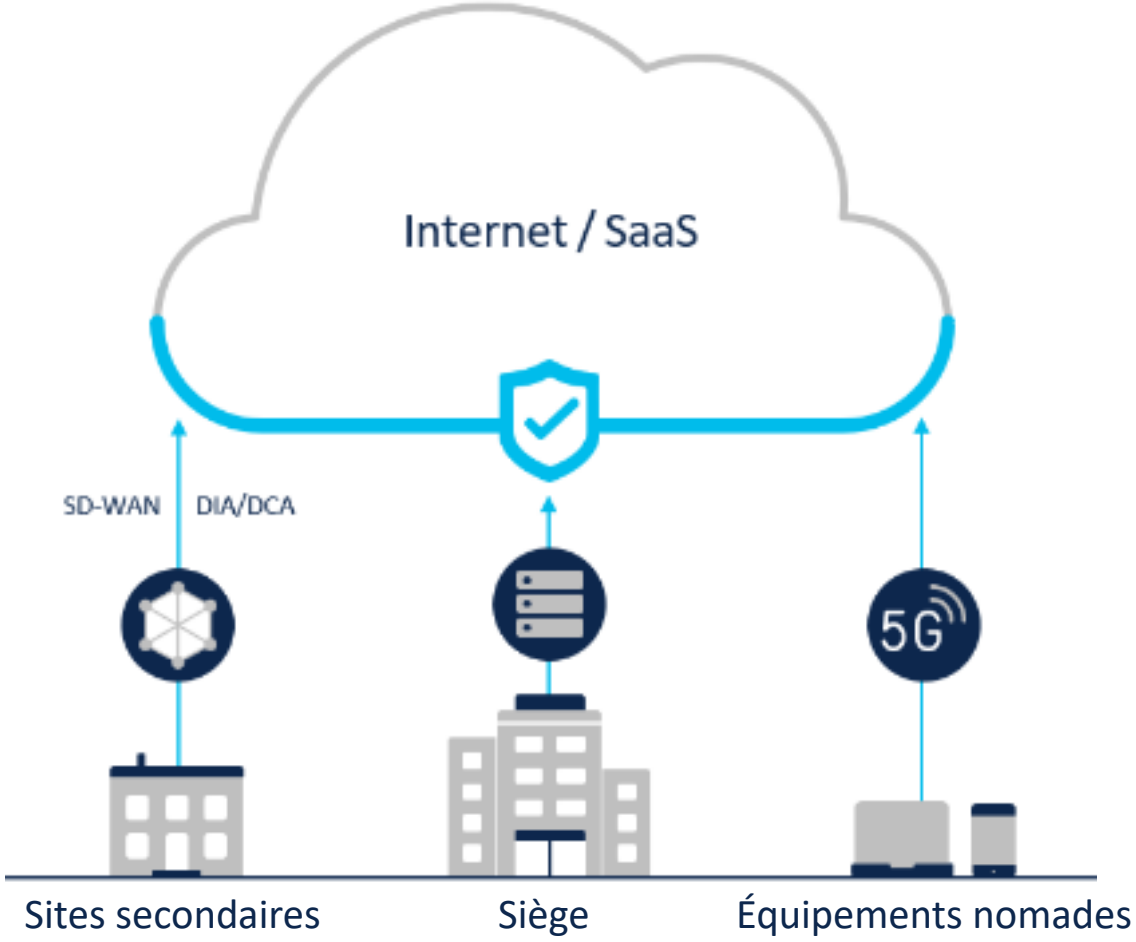
Approche Cloud

LES JOURNÉES DE LA CYBER

Sécuriser les infrastuctures et les accès

Le cloud, un outil indispensable face au risque cyber

- Centralisations et harmonisation des stratégies de sécurité
- Réductions des impacts coût vs performance
- Détection en temps réel des nouvelles menaces
- Scalabilité

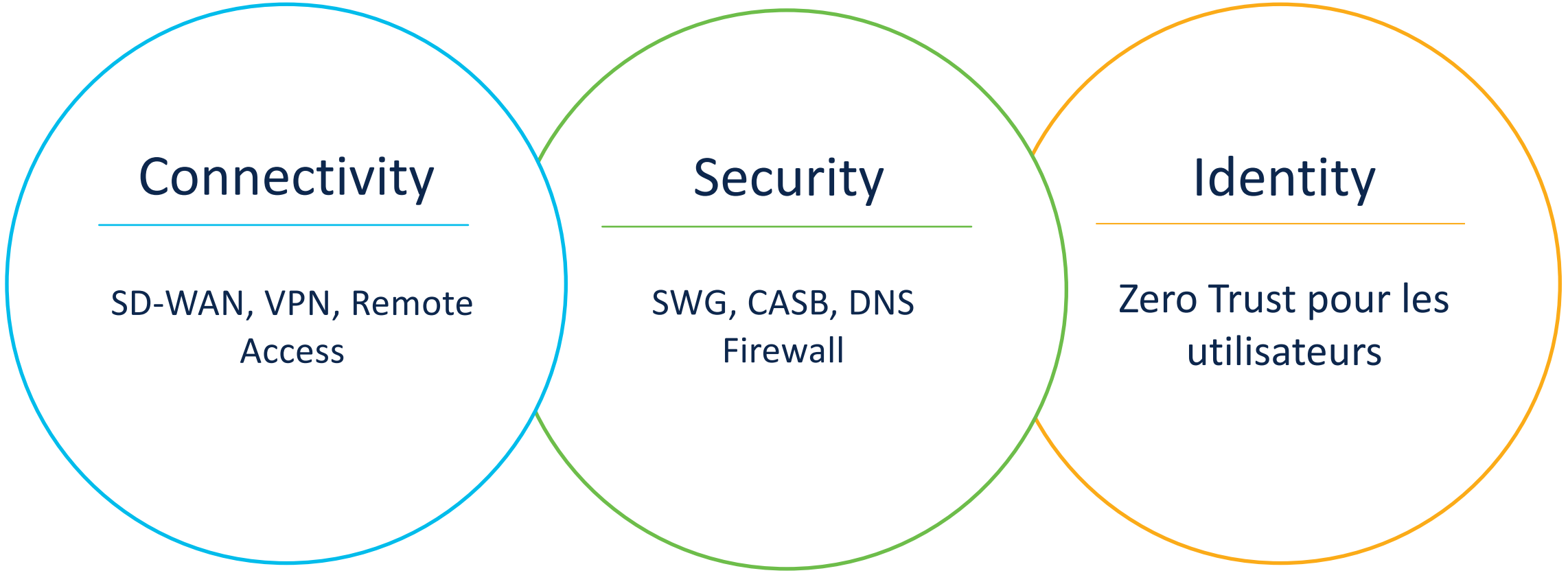


Gartner – La définition du SASE

Secure access service edge (SASE) is a **network architecture** that combines **VPN and WAN capabilities with cloud-native security** functions like secure web gateways, cloud access security brokers, firewalls, and zero-trust network access. These functions are **delivered from the cloud and provided as a service** by the SASE vendor.

Sécuriser les infrastuctures et les accès

Les 3 composants du SASE



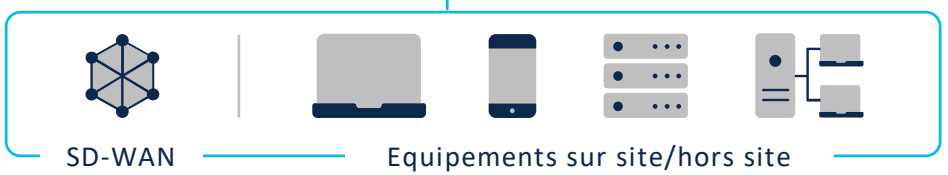
Visibilité, sécurité et intégration

LES JOURNÉES DE LA CYBER

Sécuriser les infrastuctures et les accès

Les plateformes SSE pour assurer la sécurité par le cloud

DNS-layer security	Cloud-delivered firewall	Secure web gateway	Cloud App & Data Security (CASB & DLP)	Remote Access & ZTNA	Interactive threat intel	Remote Browser Isolation
✓	✓	✓	✓	✓	✓	✓
Arrêter les menaces avant que le trafic n'atteigne mon réseau	Sécurité L7 sur l'ensemble des sites afin d'enrayer les menaces non basées sur le web.	Visibilité/contrôle complet de l'URL pour appliquer la politique et bloquer les menaces anticipées.	Découvrez, signalez et contrôlez l'utilisation des applications cloud.	Remote Access & ZTNA fournis par la plateforme de manière centralisé	Contexte de la menace en temps réel accélérant l'investigation et la réponse aux incidents	Assurer l'isolation entre le poste utilisateur et les menaces liées au navigateurs



Sécuriser les infrastuctures et les accès

Pourquoi le Zero Trust ?

1. Sécuriser des environnements hybrides et multicloud
2. Résilience face à l'évolution des attaques
3. Donner le minimum de privilege a chaque accès
4. Reduire la surface d'attaque
5. Répondre aux enjeux de conformité règlementaire

LES JOURNÉES DE LA CYBER

Sécuriser les infrastuctures et les accès

Les 3 piliers d'une stratégie Zéro Trust

Protéger les utilisateurs

Protéger les réseaux

Protéger les applications

Zero Trust Security Framework

Workforce 

Workplace 

Workloads 

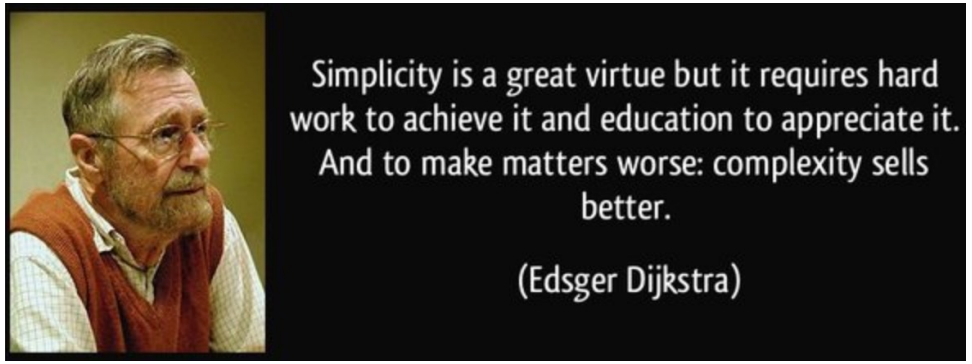
LES JOURNÉES DE LA CYBER

Modéliser, Déployer et Sécuriser automatiquement vos systèmes dans le Cloud

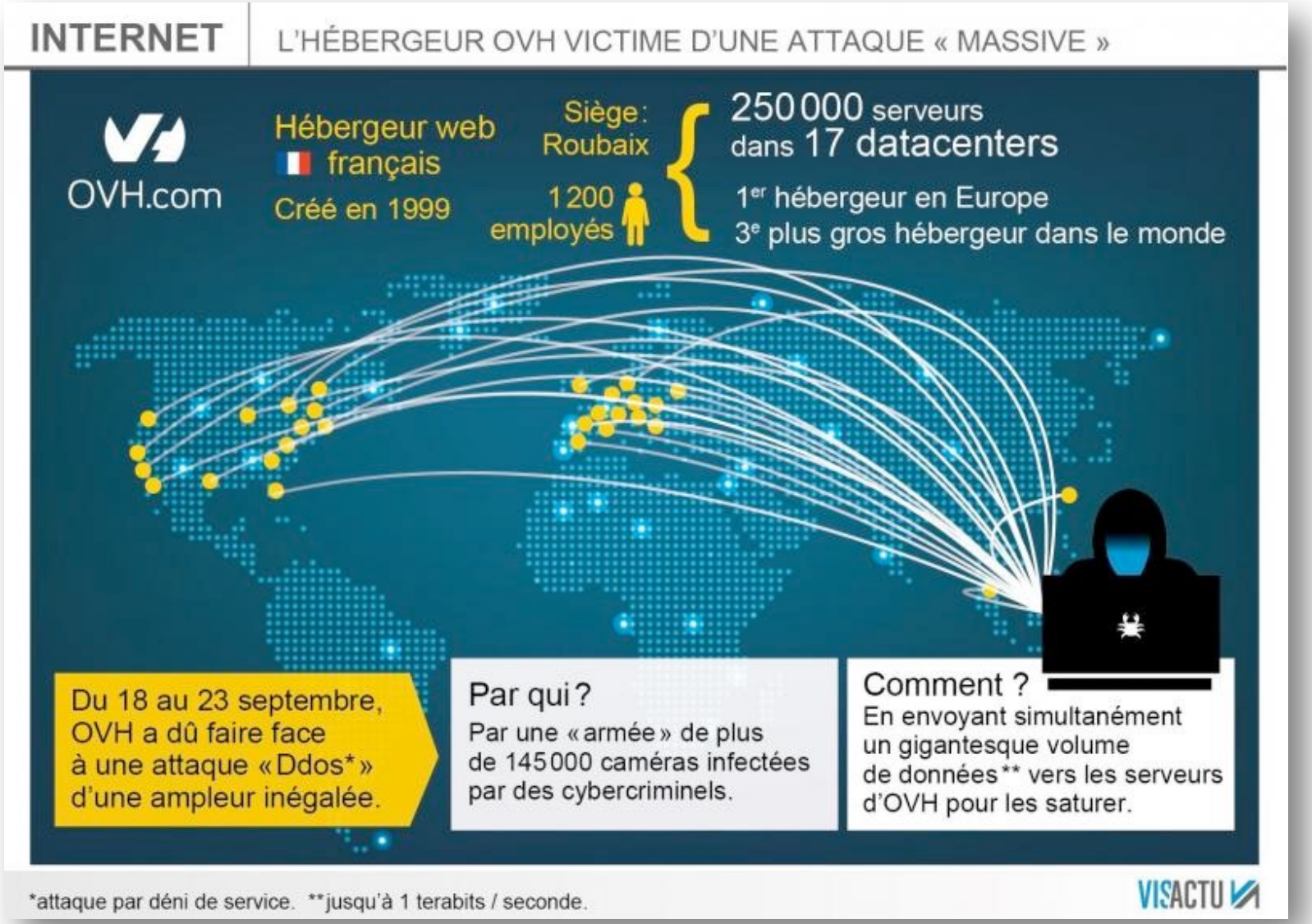
- Start'up Inria, ENS de Lyon, CNRS, UCB Lyon 1
  - Une Approche basée sur la transformation de modèles
- Un accompagnement dédié de la conception/modélisation au déploiement
- Des solutions de sécurité (système, logiciel ou réseau (ex: CISCO)) à leur mise en œuvre
- http://www.qirinus.com

Le Cloud, LA solution face aux risques cyber ?

- Des Infrastructures Sécurisées
- La garantie de logiciels Sécurisés
- Isolation garantie par la Virtualisation
- En cas d'attaque la garantie de toucher les dommages-intérêts
  - Tarif minimum et moyen: 0€
  - Tarif maximum: Un montant égal à un an de frais (rétrocédé)
- SECaaS : SECurity as a Service … reste « juste » un « peu » de configuration à finaliser

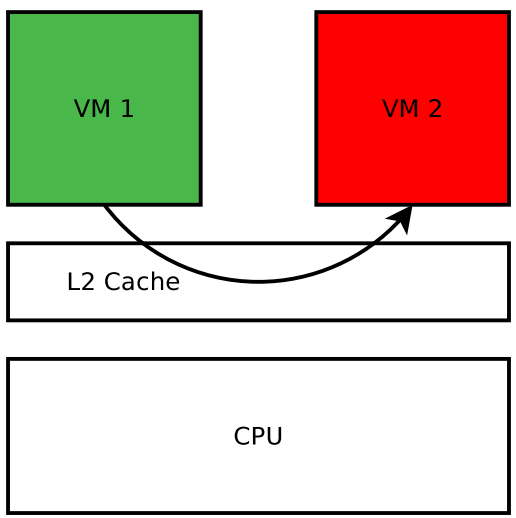


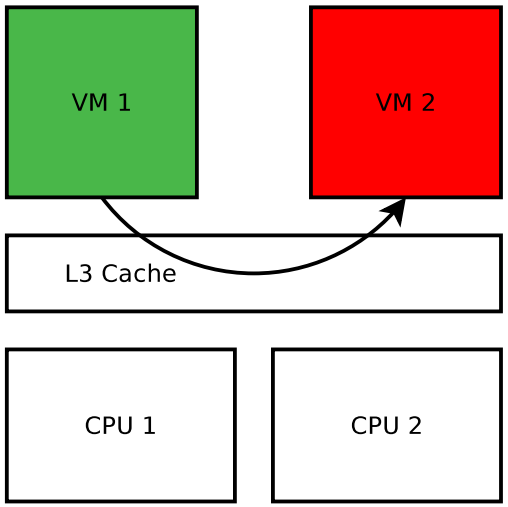
Derrière la caméra…

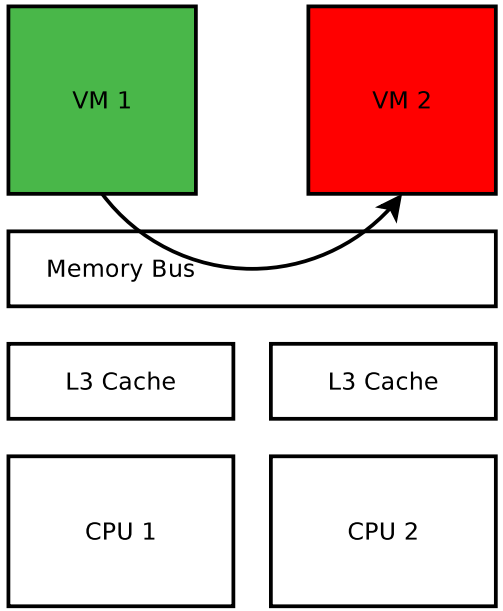


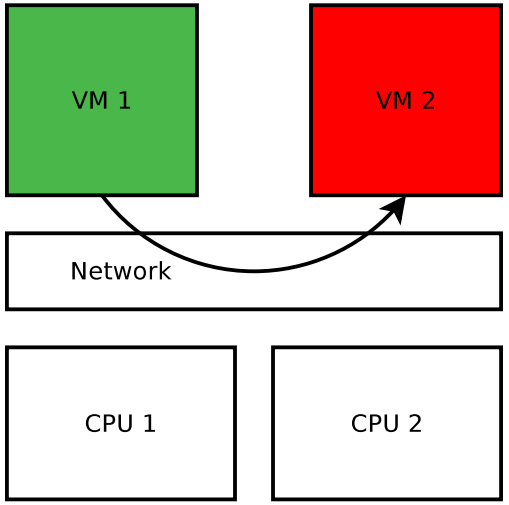
Pas si seul …

- La sécurisation d'une machine isolée ne peut garantir la sécurité Cloud dans les infrastructures virtualisées (*side channel attack*)
- **La virtualisation n'est pas la sécurité !**





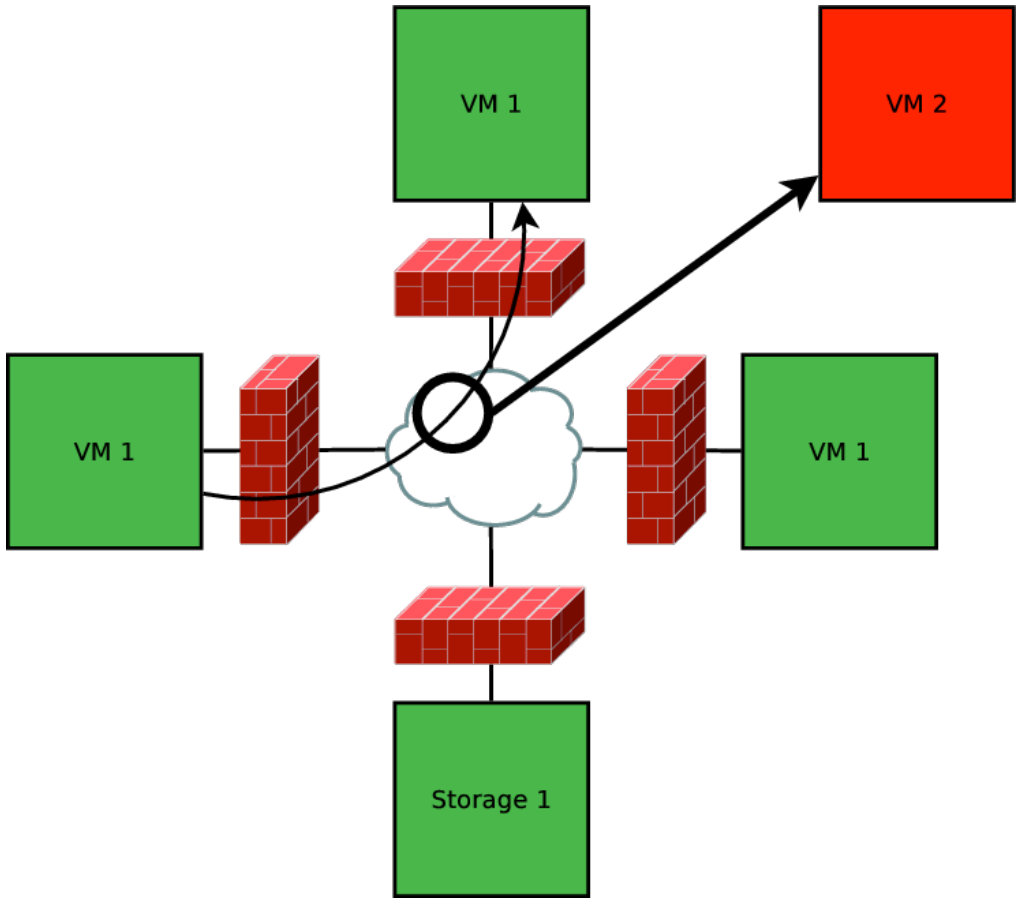




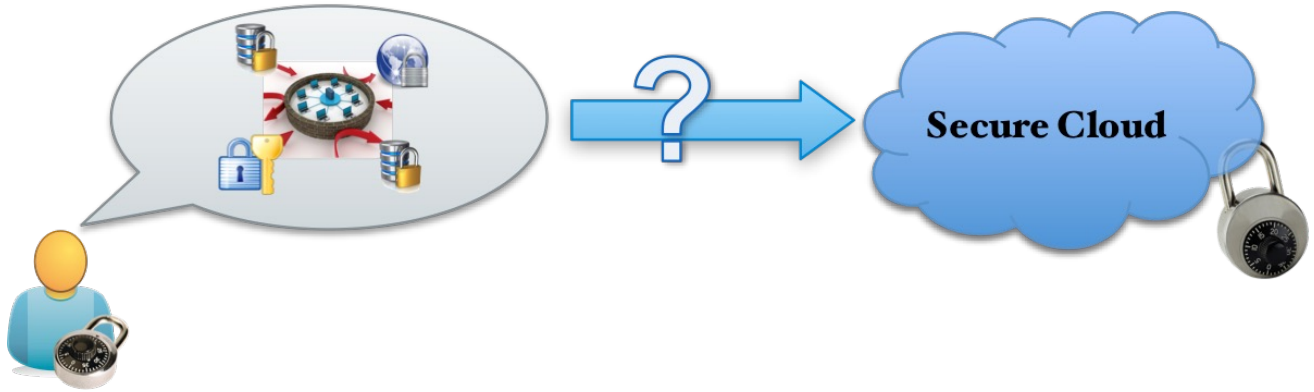
M. Christodorescu, R. Sailer, D. L. Schales, D. Sgandurra, and D. Zamboni. Cloud security is not (just) virtualization security. In Proc. of the 2009 ACM workshop on Cloud computing security

Pas si seul et même trop nombreux…

- L'isolation des machines virtuelles n'est pas suffisante pour la sécurité
- Le défi n'est pas juste de sécuriser une application sur une machine mais de garantir la sécurité d'un ensemble de machines vue comme une seule entitée.
- Les serveurs de sécurité centralisés ne seront pas efficace



Objectifs de sécurité pour le Cloud

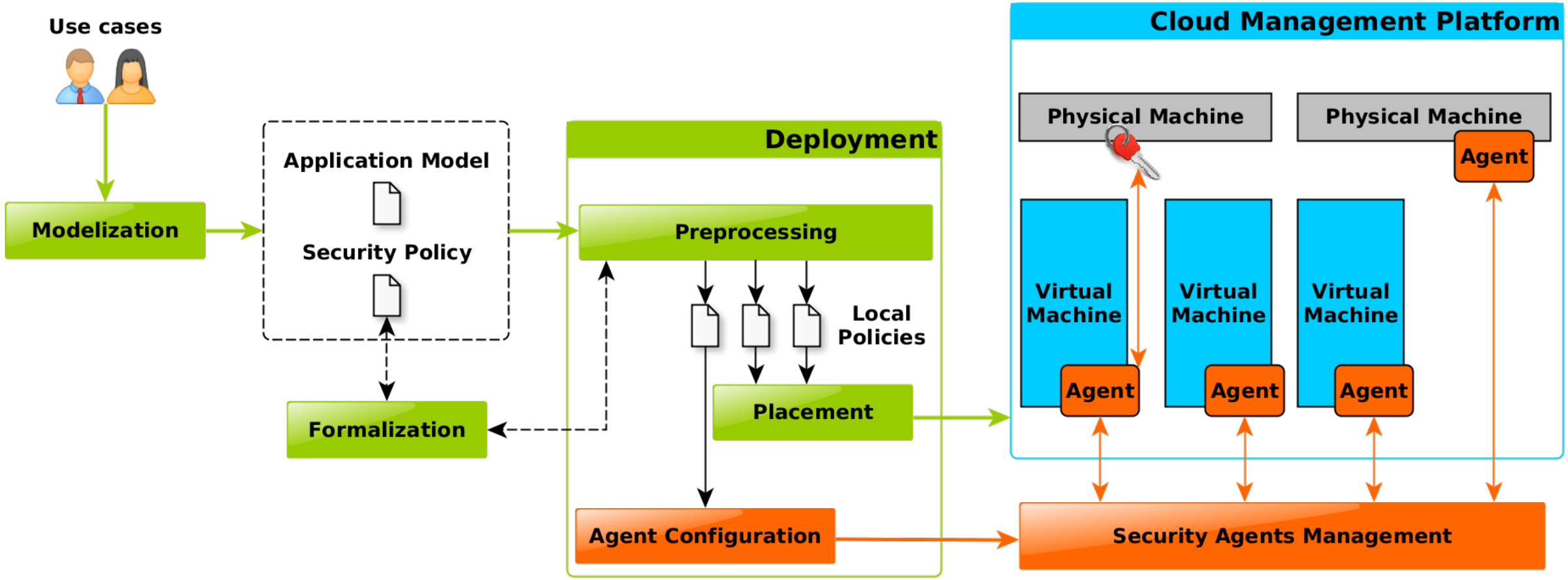


- Motivation [Sandhu'10]: "Need to develop models, methodologies and architectures for decentralized dynamic management of security and assurance policies"

- Contribution: Fournir un modèle d'application Cloud et la politique de sécurité associée pour concevoir des algorithmes d'ordonnancement/de provisionnement tenant compte de la sécurité (étape de décision).

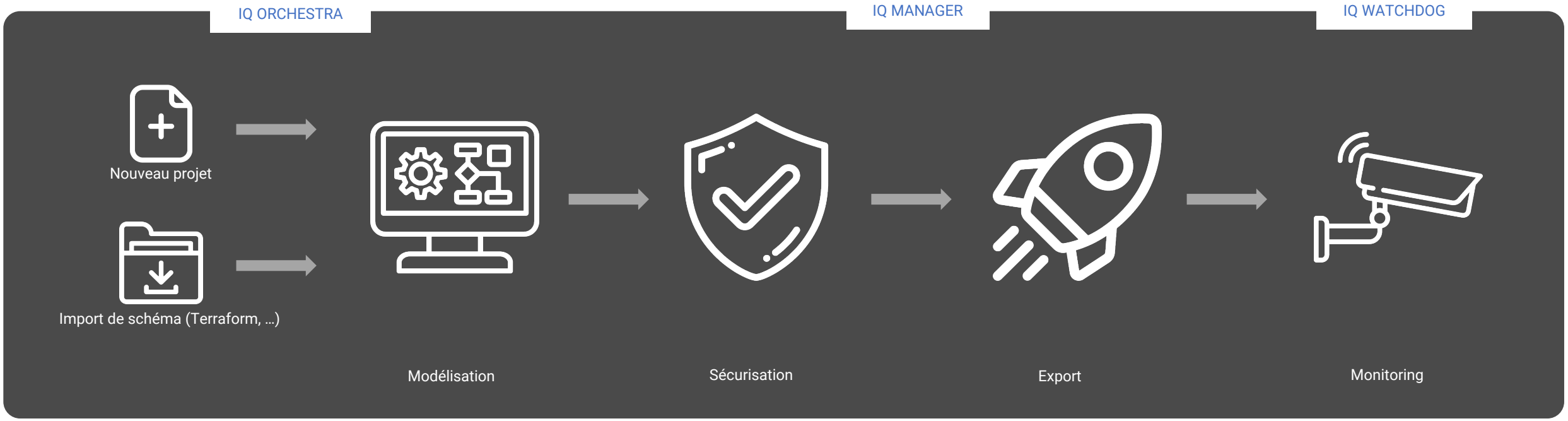
- Objectif à long terme : Exploiter des modèles sensibles à la sécurité pour fournir un déploiement et une configuration automatiques de la sécurité dans le Cloud (étape de distribution et de projection).

Big Picture


Use cases
Modelization
Application Model
Security Policy
Formalization
Deployment
Preprocessing
Local Policies
Placement
Agent Configuration
Cloud Management Platform
Physical Machine
Physical Machine
Agent
Virtual Machine
Virtual Machine
Virtual Machine
Agent
Agent
Agent
Security Agents Management

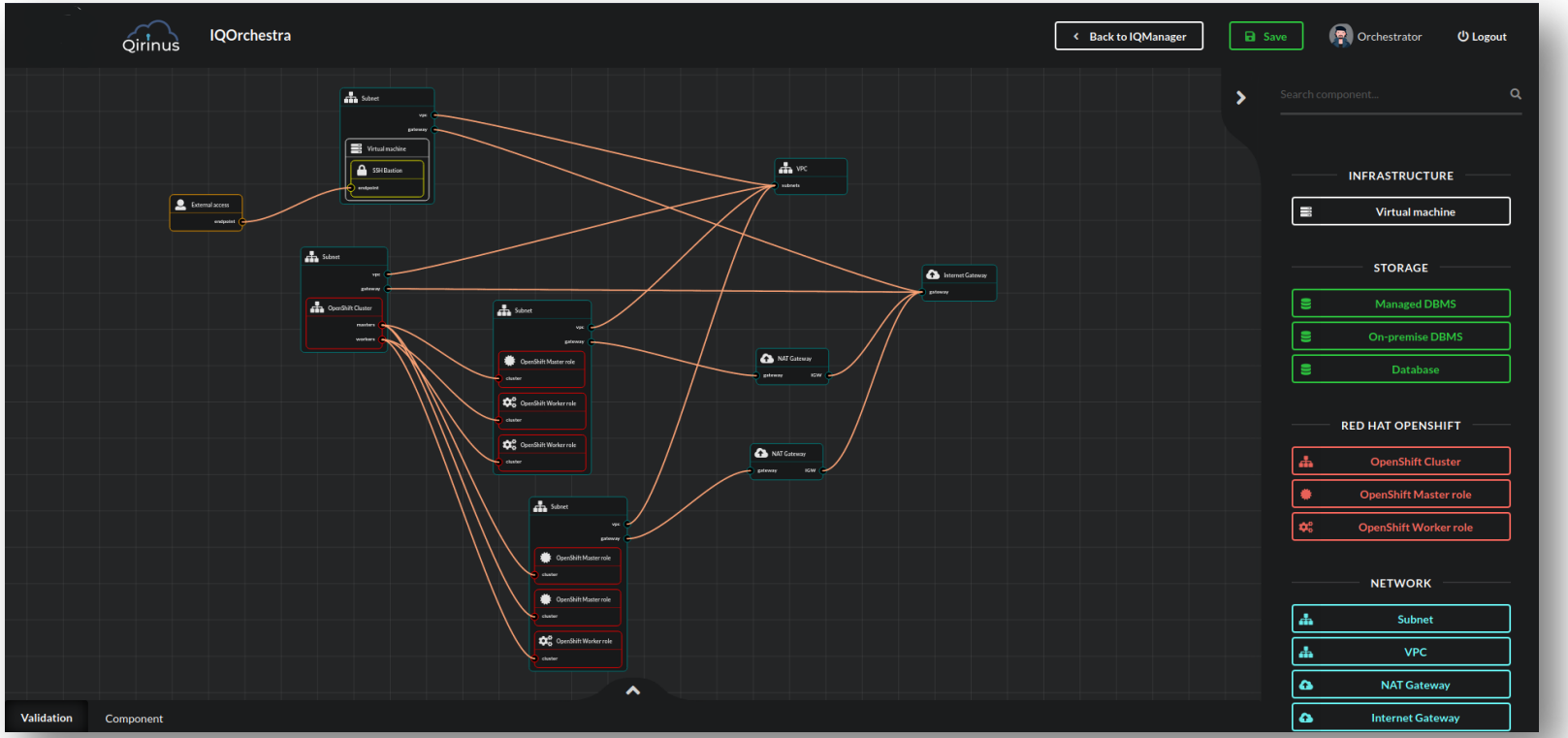
Le workflow Qirinus

- un orchestrateur unique issue de la recherche capable de modéliser, déployer, sécuriser l'infrastructure et les applications



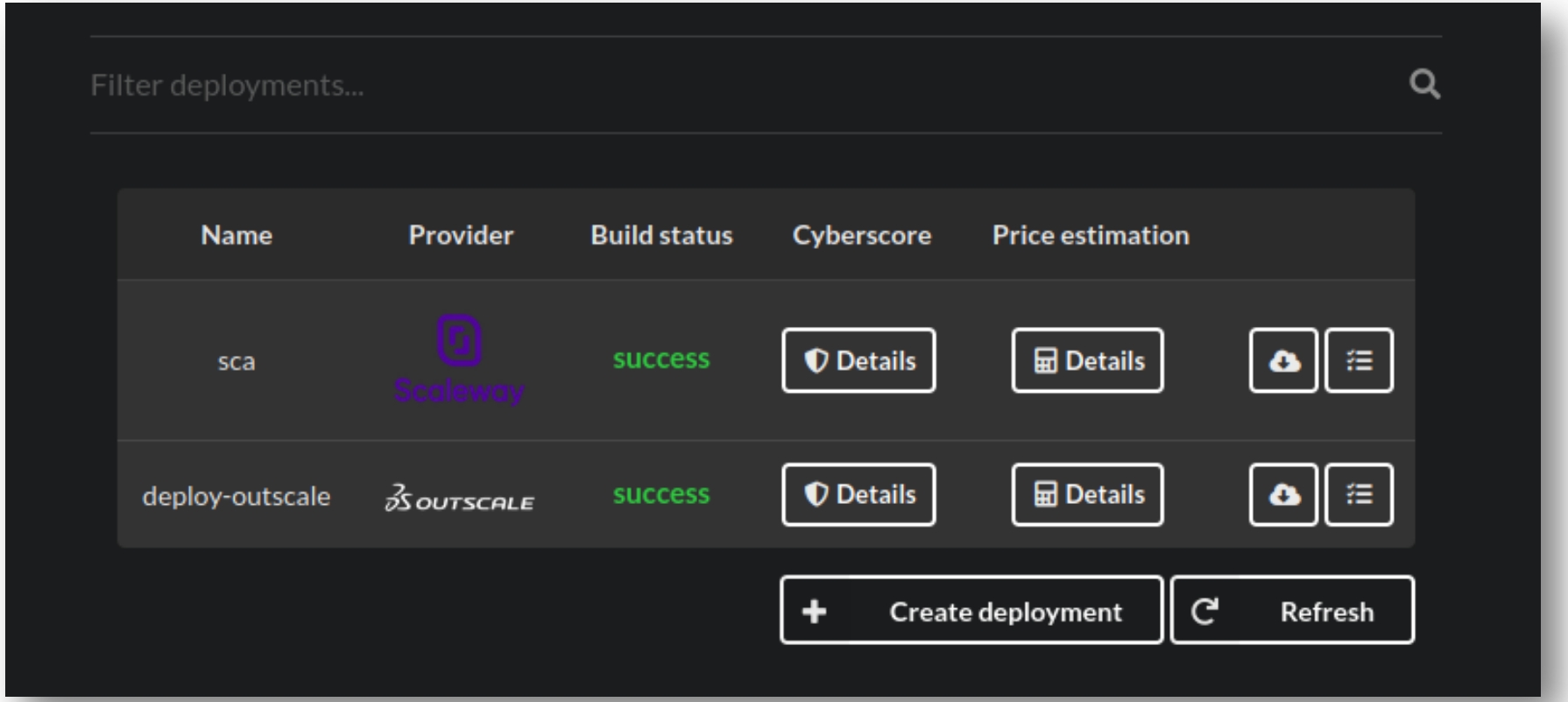
La modélisation via le Designer

- Conception du déploiement
- Création de nouveaux composants dans le Designer



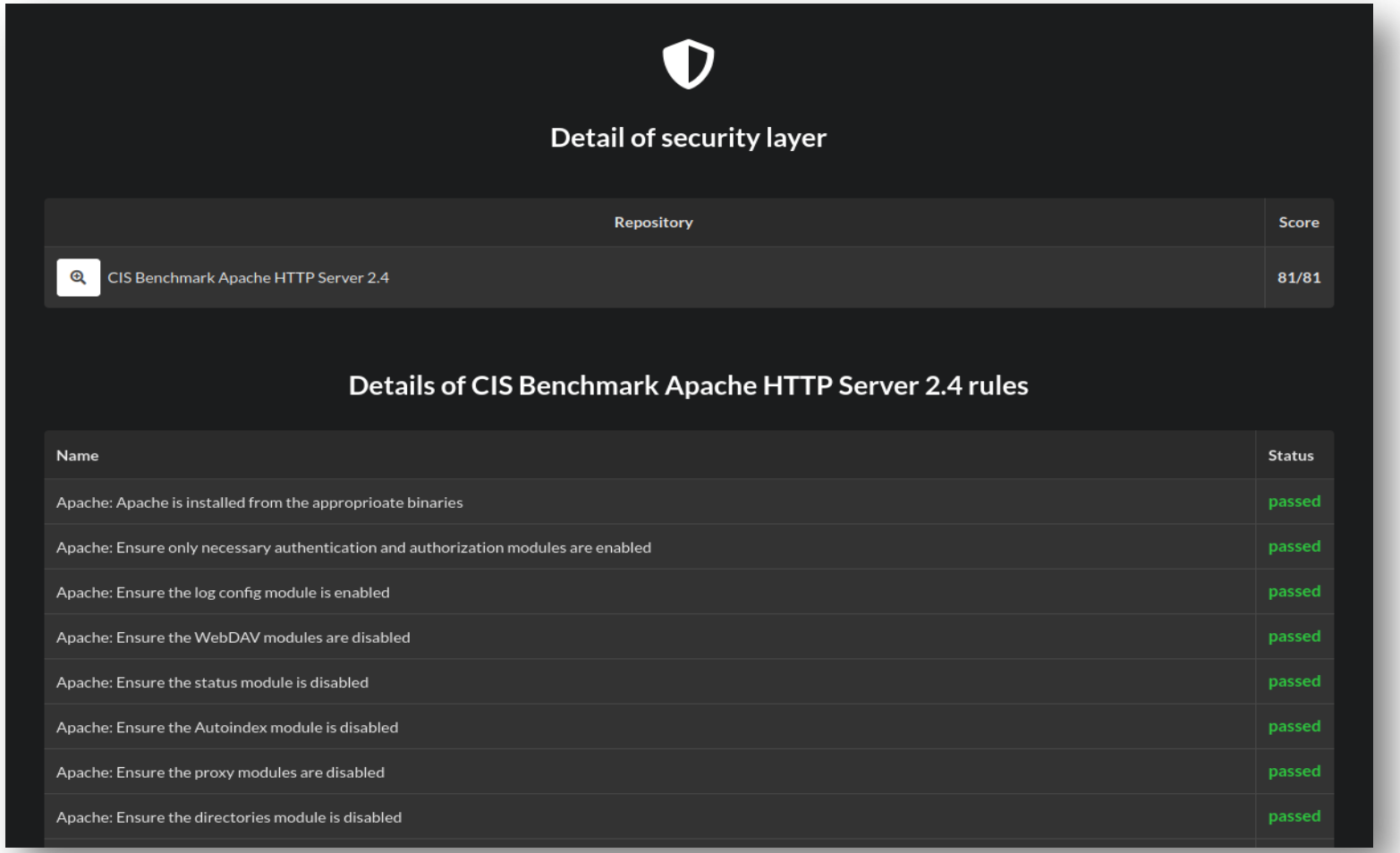
Le déploiement: IQmanager

- Cloud agnostique
  - Proposition automatique des Cloud provider candidats
  - Cloud: AWS, Azure, Outscale, Scaleway, etc.



Le Cyberscore

- Mesure qualitatif du niveau de sécurité et validation automatique
  - Ex: CIS Benchmark



Detail of security layer

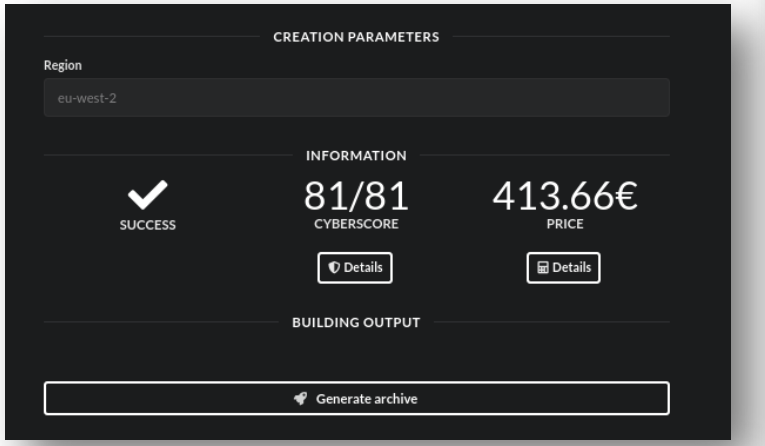
Repository	Score
CIS Benchmark Apache HTTP Server 2.4	81/81

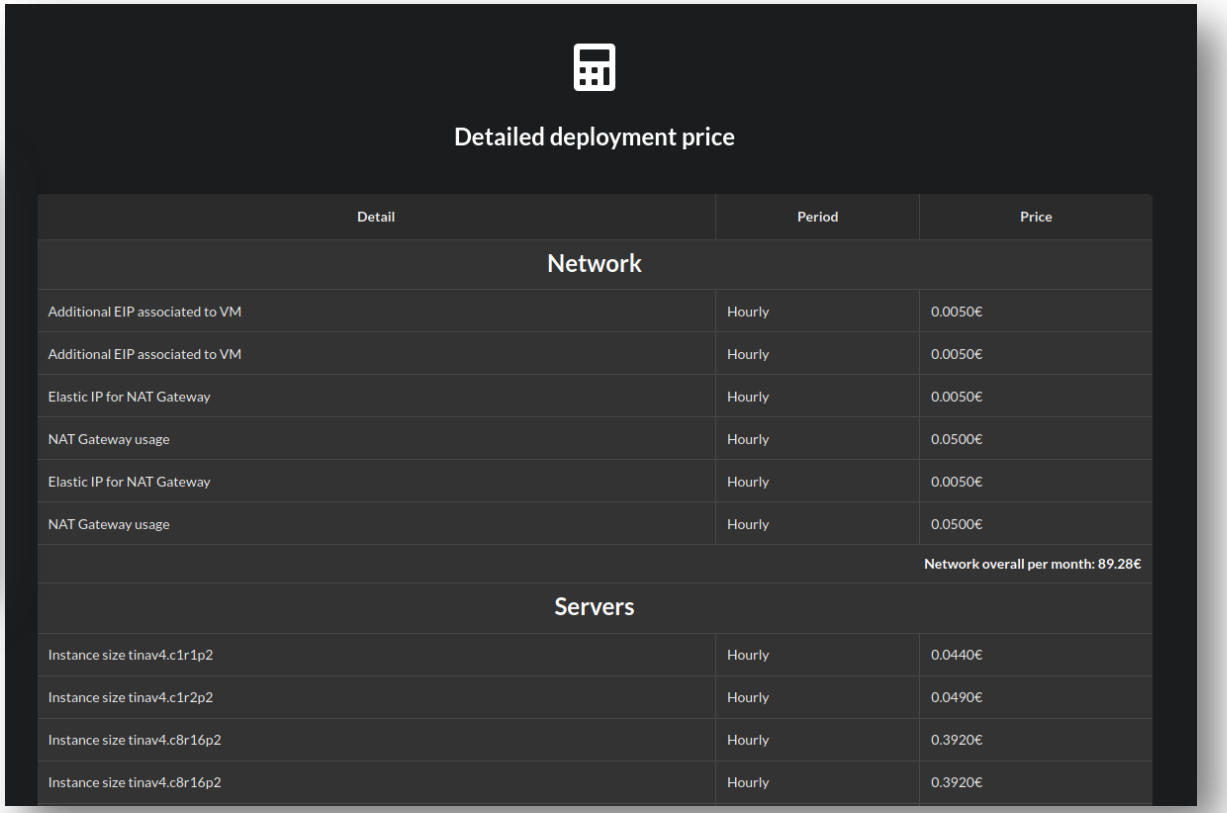
Details of CIS Benchmark Apache HTTP Server 2.4 rules

Name	Status
Apache: Apache is installed from the approprioate binaries	passed
Apache: Ensure only necessary authentication and authorization modules are enabled	passed
Apache: Ensure the log config module is enabled	passed
Apache: Ensure the WebDAV modules are disabled	passed
Apache: Ensure the status module is disabled	passed
Apache: Ensure the Autoindex module is disabled	passed
Apache: Ensure the proxy modules are disabled	passed
Apache: Ensure the directories module is disabled	passed

Le Pricing

- Devis automatique pré-déploiement





Detailed deployment price

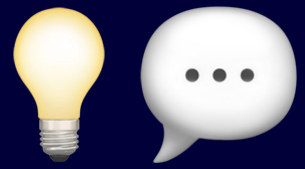
Detail	Period	Price
Network		
Additional EIP associated to VM	Hourly	0.0050€
Additional EIP associated to VM	Hourly	0.0050€
Elastic IP for NAT Gateway	Hourly	0.0050€
NAT Gateway usage	Hourly	0.0500€
Elastic IP for NAT Gateway	Hourly	0.0050€
NAT Gateway usage	Hourly	0.0500€
		Network overall per month: 89.28€
Servers		
Instance size tinav4.c1r1p2	Hourly	0.0440€
Instance size tinav4.c1r2p2	Hourly	0.0490€
Instance size tinav4.c8r16p2	Hourly	0.3920€
Instance size tinav4.c8r16p2	Hourly	0.3920€

Conclusions

- Les Infrastructures virtualisées pour vos déploiements sécurisés: une bonne approche ?
  - Oui mais … pas si simple !

- Qirinus propose un orchestrateur de sécurité pour les infrastructures virtualisés
  - Une solution issue de plusieurs années de recherche
  - Un orchestrateur fortement configurable (approche par modèles)
  - Configuration automatique des solutions de sécurité système, logiciel et réseau (ex: CISCO)

- Travaux futurs
  - Gestion du cycle de vie pour l'optimisation des dépenses Cloud
  - IQ WATCHDOG : Prise en compte des CVE et détections des failles



LES JOURNÉES DE LA CYBER