Mobile and cloud security

Esercitazione

> Gianpiero Costantino

> 2017 $ CyberSecurity Master

02/09/2017

$ Info

- Saranno 6 ore di esercitazione sul Cloud Computing;
- Metteremo in pratica alcuni aspetti visti durante le ore di lezione:
  - Gestione del Cloud pubblico;
  - Utilizzo del Cloud attraverso istanze virtuali;
  - Sicurezza nel Cloud;

$ Test

- Usiamo la piattaforma online **Kahoot**!

- Collegatevi su https://kahoot.it
- Mettete il vostro *Nome* e *Cognome* (**non fate i furbi**)

$ Breve riepilogo sul Cloud

Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services).

These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization.

This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs.

Tratto da:

L.M. Vaquero, L. Rodero-Merino, J. Caceres, M. Lindner: "A Break in the Clouds: Towards a Cloud Definition", 2008

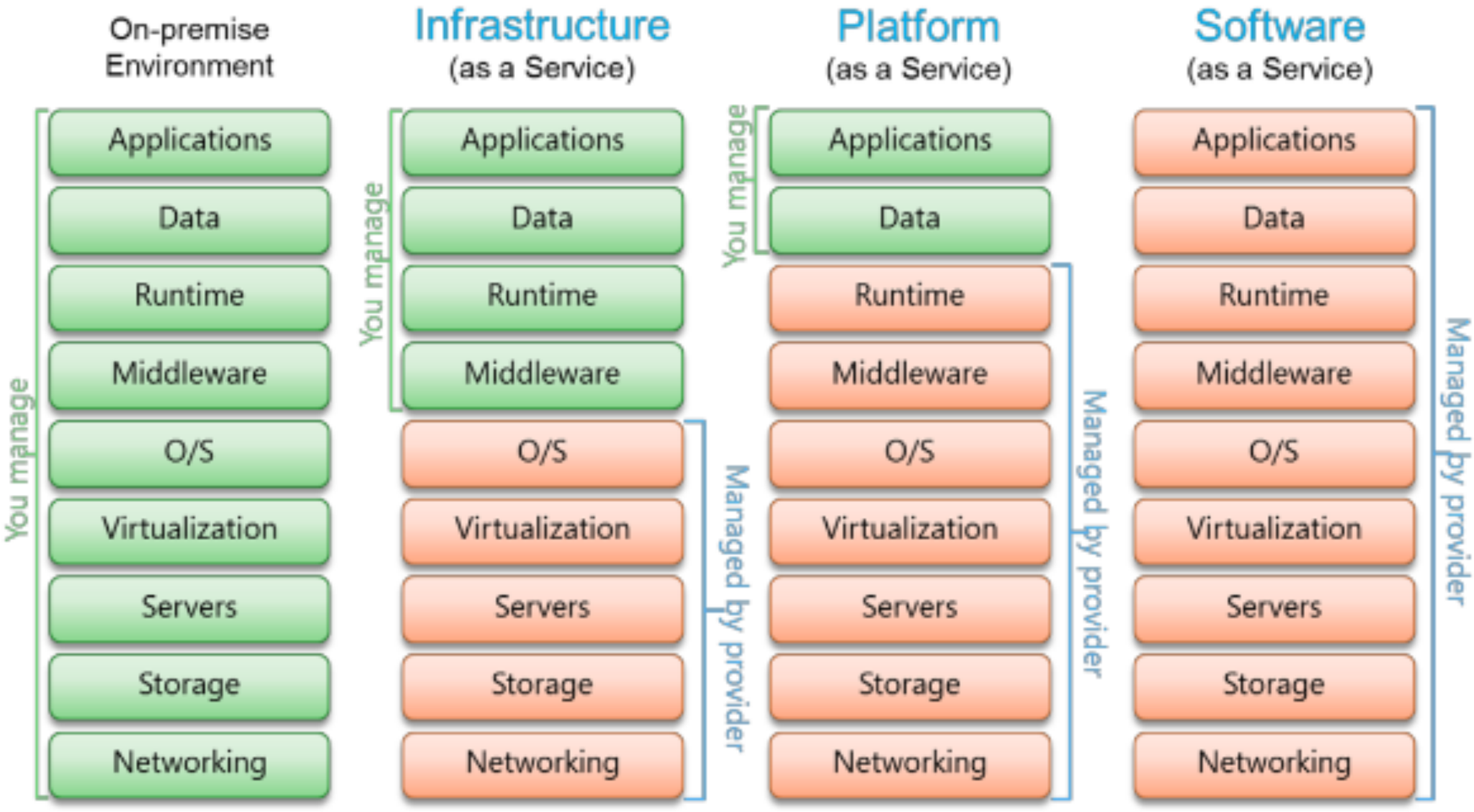
$ Breve riepilogo sul Cloud

- Alcune caratteristiche fondamentali:
  - Self-service su richiesta
  - Ampio accesso alla rete
  - Risorse comuni
  - Elasticità rapida
  - Affidabilità
  - Disponibilità

$ Modelli di Servizio

- **Infrastructure as a Service** (IaaS)
  - Infrastruttura computazionale (calcolo, storage, network)
- **Platform as a Service** (PaaS)
  - Infrastruttura su cui installare ed eseguire applicazioni sviluppate utilizzando strumenti supportati dal provider (ad es, linguaggi, librerie)
- **Software as a Service** (SaaS)
  - Utilizzo di applicazioni del provider su infrastruttura Cloud

$ Modelli di Servizio



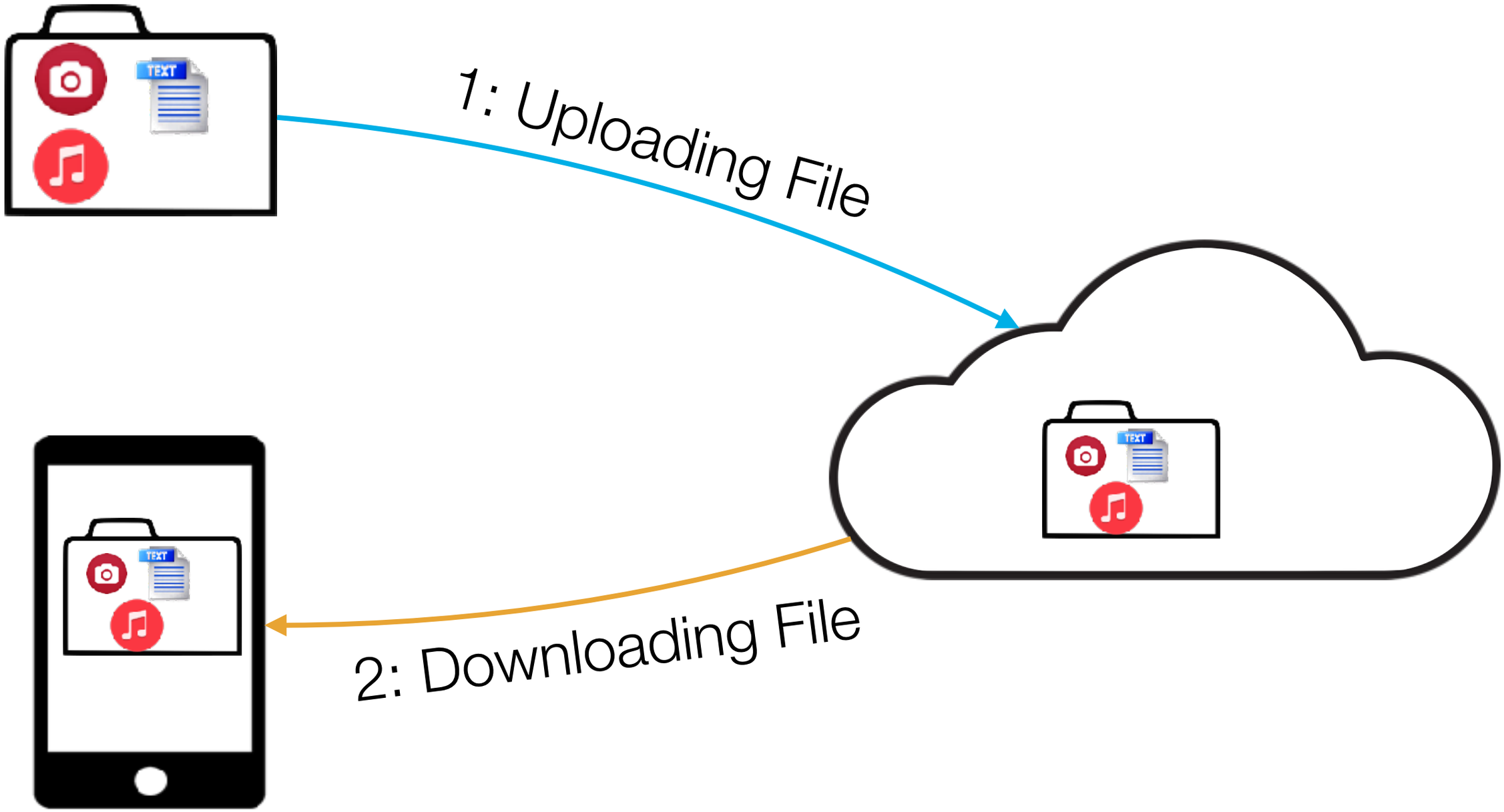
$ Modelli di deployment

- **Cloud Pubblico:**
  - A chiunque ne faccia richiesta (spesso a pagamento)
- **Cloud Privato:**
  - Ad un insieme di utenti predefinito (e.g., organizzazione)
- **Cloud Ibrido:**
  - Combinazione di Pubblico e Privato

$ Pubblico Vs Privato

amazon web services		openstack
Chiunque	**Utenti**	Membri di una organizzazione
Cloud Provider	**Operato da**	Organizzazione che lo utilizza Terza parte fidata
Internet	**Rete**	Privata Internet
Non Confidenziali	**Adatto per Dati e Processi**	Confidenziali (dati sensibili, personali, segreti, di valore)

$ Privacy nel Cloud



$ Privacy nel Cloud

- Cloud Provider come Dropbox, Google Drive, e altri caricano i vostri dati nel cloud “in chiaro”;

- File sensibili potrebbero essere letti dai cloud provider senza che voi lo sappiate;

$ BoxCryptor

boxcryptor non si tratta di un cloud provider, ma consente di codificare i vostri file prima di caricarli sul cloud

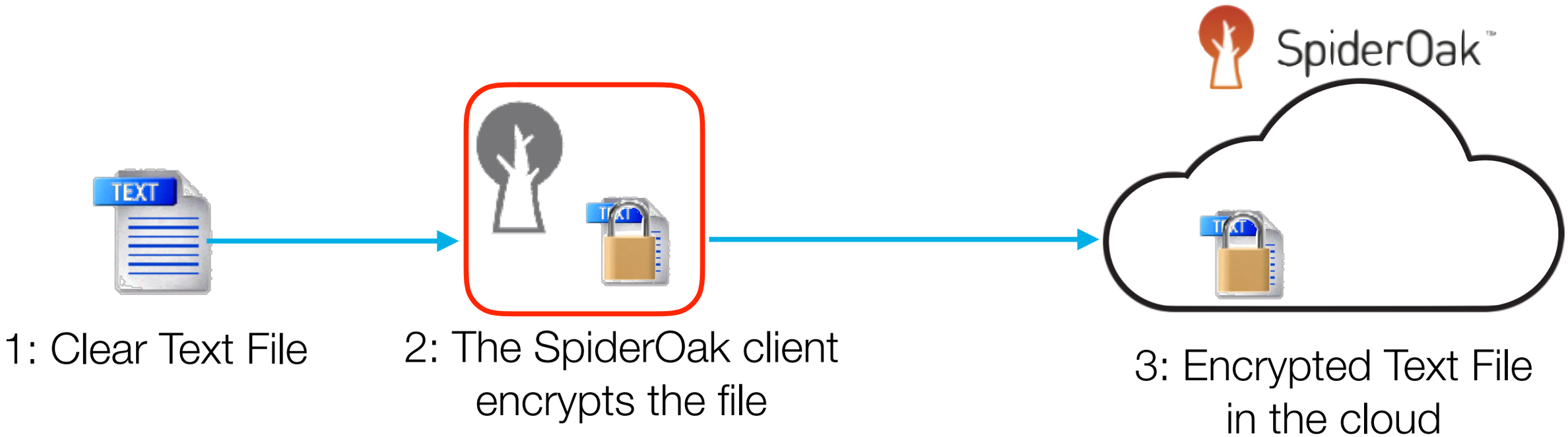
1: Clear Text File

2: It encrypts the Text File

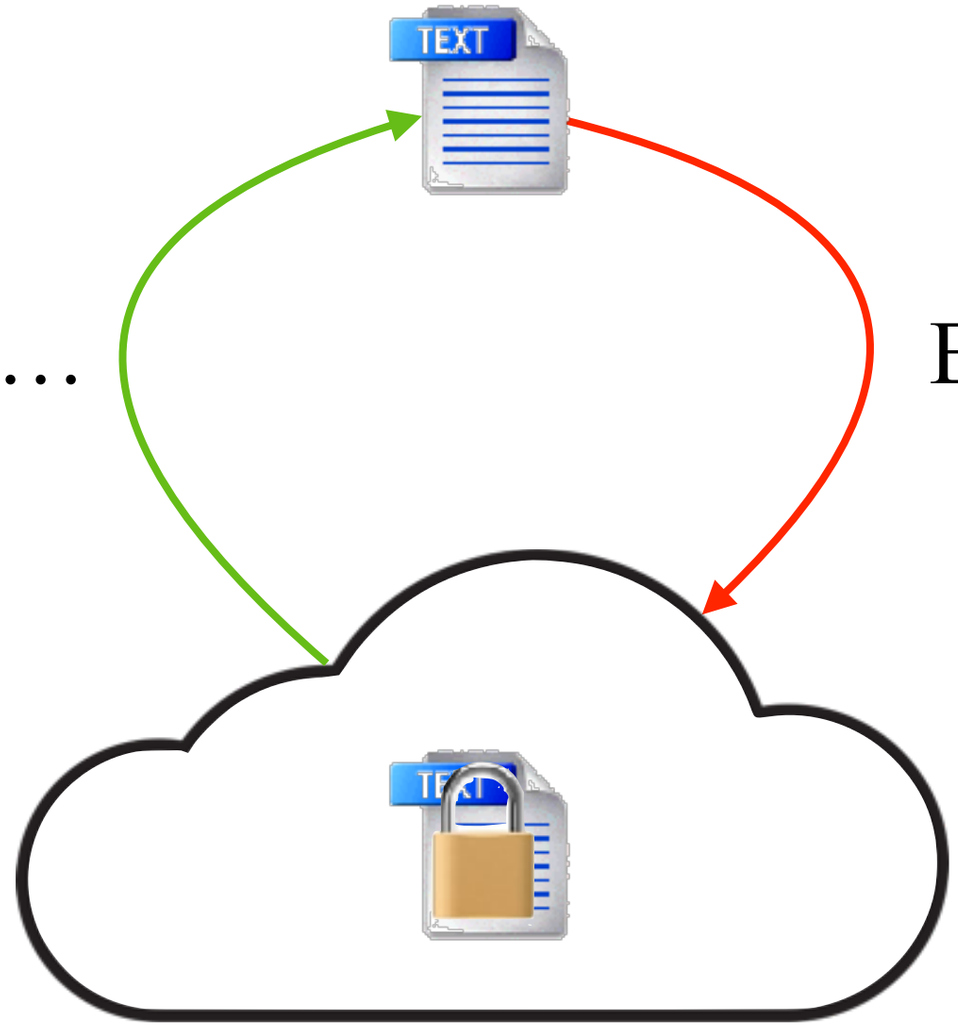
3: Encrypted Text File into your cloud providers

$ SpiderOak

SpiderOak™ è cloud provider



$ Svantaggi…



$ Altre soluzioni?

- La domanda è:

Posso usare una soluzione diversa per proteggere i miei dati nel cloud?

Lavorare sui [illegible]ttografati?!?!?!

$ Presente e futuro

- **Homomorphic Encryption** è una recente tecnica crittografica che permette di effettuare operazioni su dati crittografati come se questi fossero in chiaro;

HC@WORKS

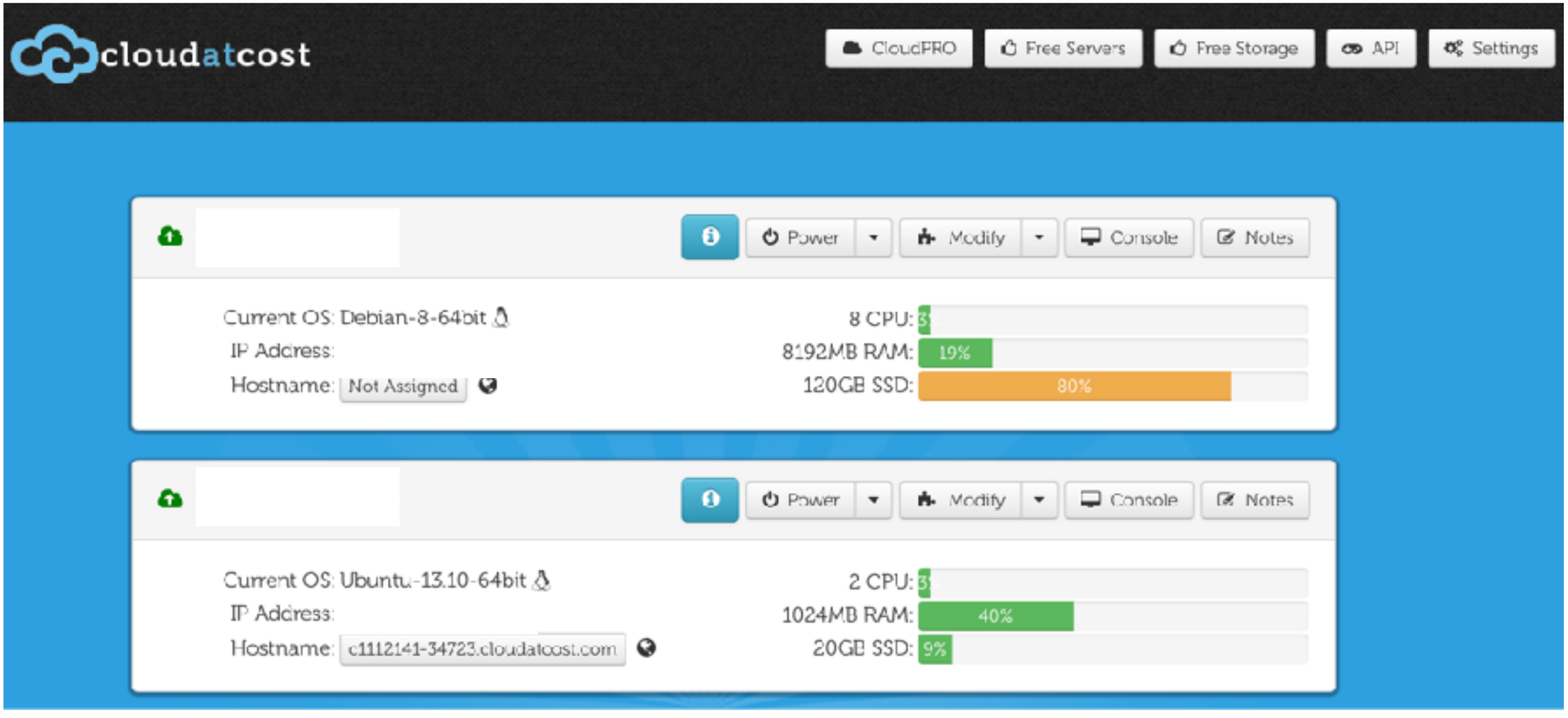
$ Andiamo sul pratico…

- **Cloudatcost:**
  - è **pubblico**;
  - vende istanze virtuali;
    - una tantum o in abbonamento;
  - Utilizzo semplice attraverso un **pannello** web
  - Non offre un servizio impeccabile per quanto riguardo *affidabilità* e *disponibilità*

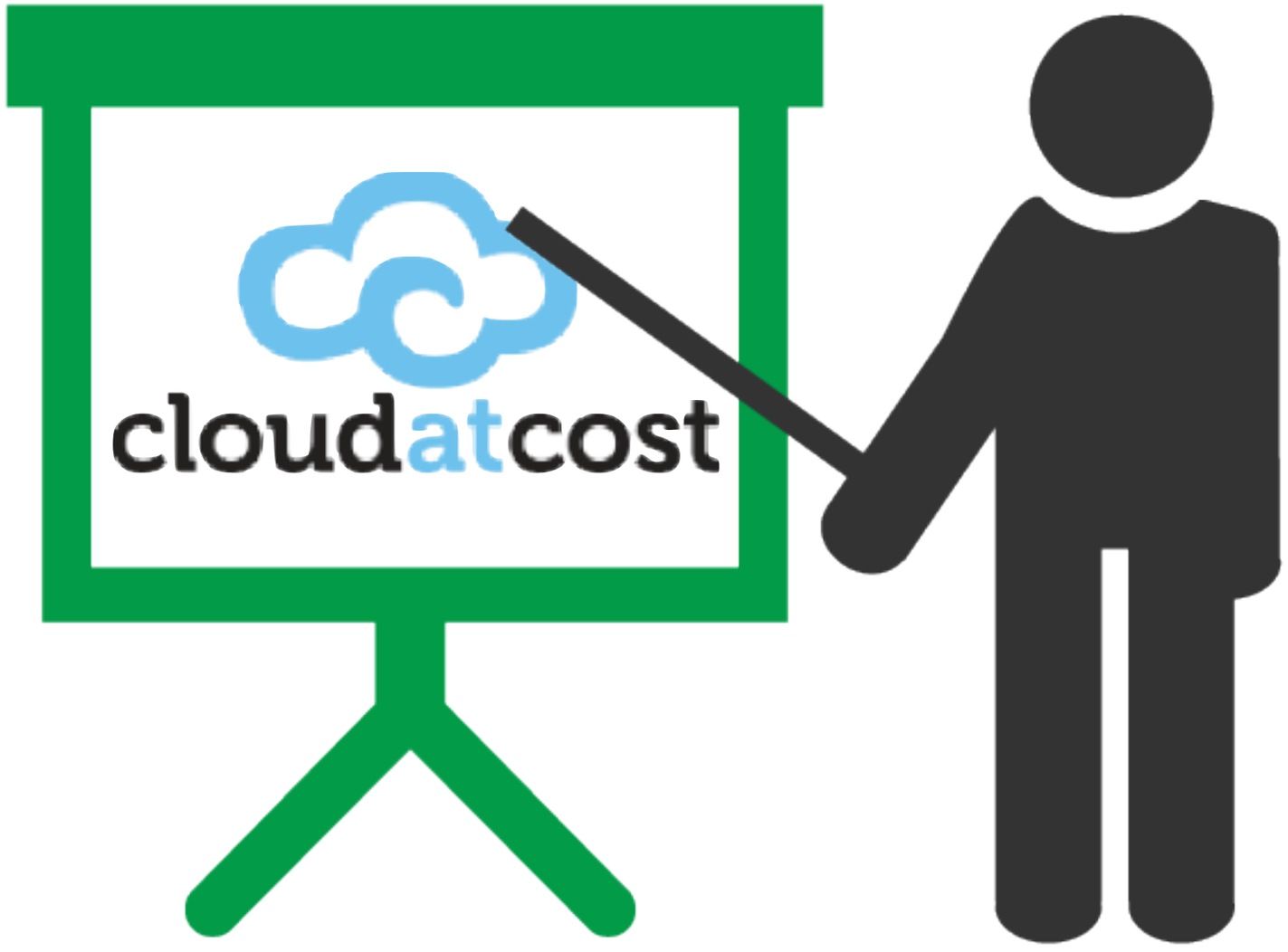
Developer CloudPRO 1	Developer CloudPRO 2	Developer CloudPRO 3
$35/one time *	$70/one time *	$140/one time *
1 vCPU Core	2 vCPU Core's	4 vCPU Core's
2 public IP per Server	2 public IP per Server	2 public IP per Server
512MB ECC RAM	1GB ECC RAM	2GB ECC RAM
10GB SSD	20GB SSD	40GB SSD
1 Gbit Network	1 Gbit Network	1 Gbit Network
unmetered monthly transfer	unmetered monthly transfer	unmetered monthly transfer

$ Andiamo sul pratico…

https://panel.cloudatcost.com



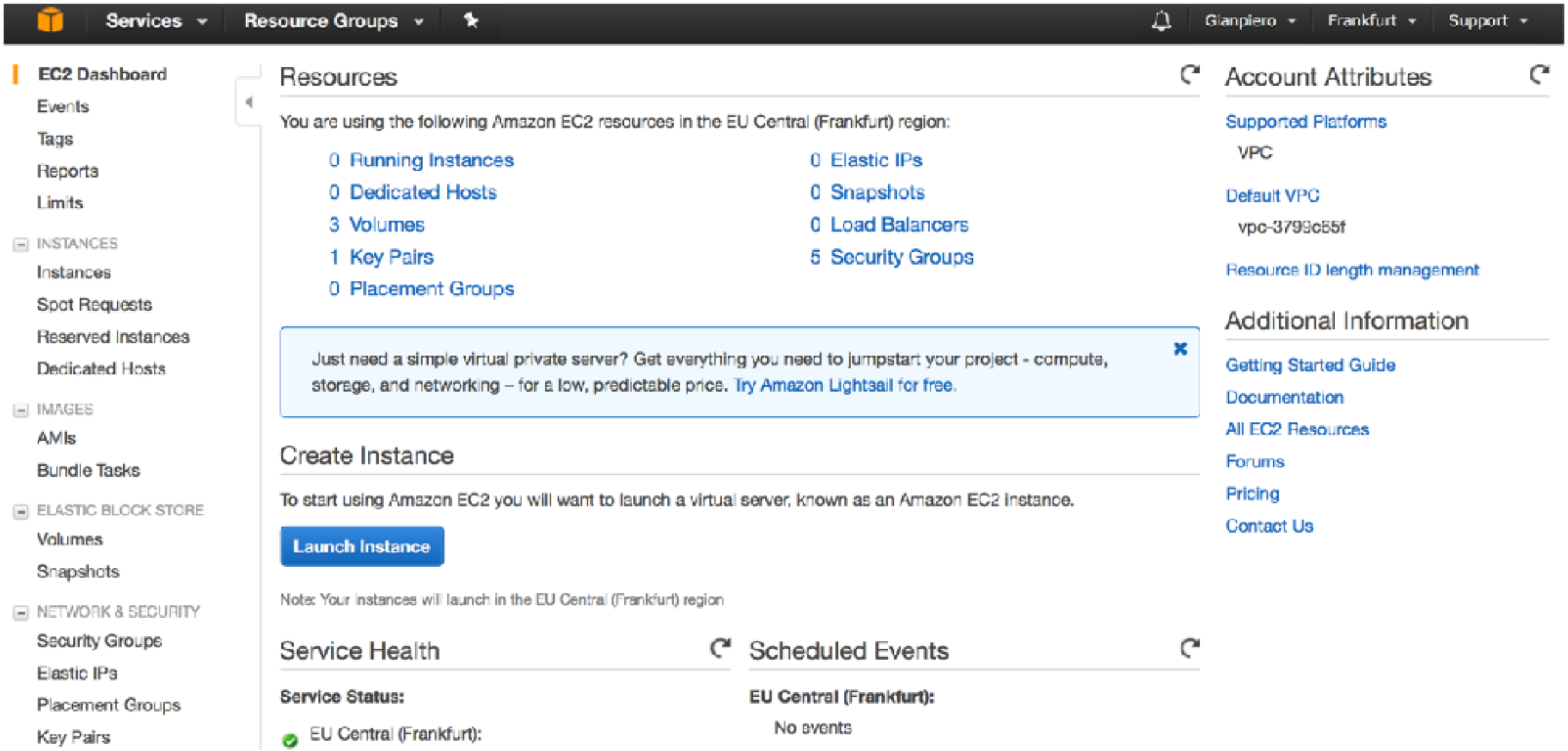
$ Dimostrazione



$ Amazon AWS

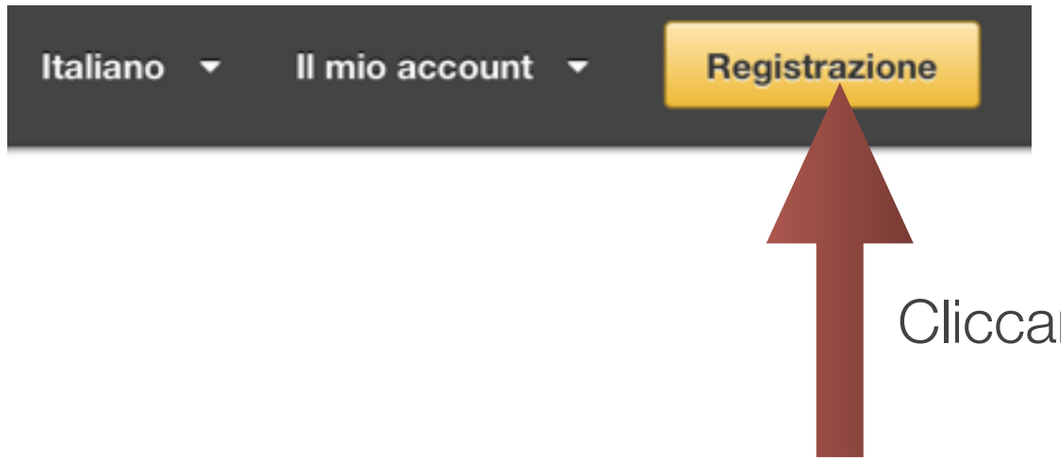
- **Amazon Web Services (EC2):**
  - è un cloud pubblico;
  - modello di servizio **IaaS**;
  - molto più completo di Cloudatcost e offre tantissimi servizi;
    - *istanze virtuali;*
    - *spazio disco;*
    - *tool per database;*
    - *e tanto altro.*
  - Utilizzo attraverso un pannello web;
  - A pagamento dipendentemente dalle risorse acquistate;

$ Elastic Compute Cloud (EC2)



$ Registrazione su AWS

- Andate su https://aws.amazon.com/it/console/



- Piano gratuito per 12 Mesi

Elastic Compute Cloud (EC2)

- 750 ore di uso di istanze Amazon EC2 t2.micro per Linux (1 GiB di memoria e supporto per piattaforme a 32 bit e a 64 bit) – sufficienti per l'esecuzione continua ogni mese*

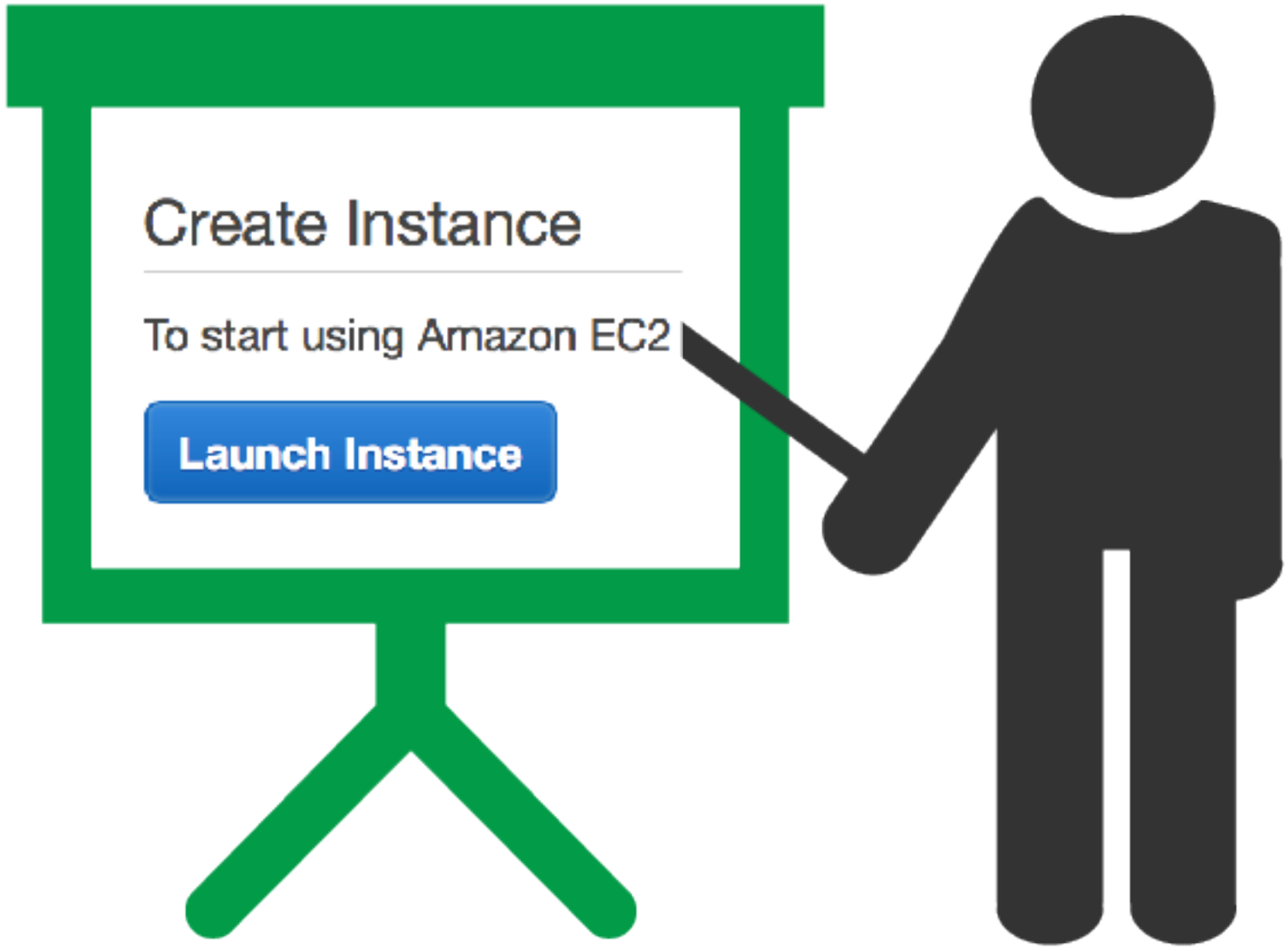
Serve carta di credito valida

Serve numero di telefono per identificazione e necessarie 24h per attivazione completa

$ Creare un’istanza virtuale

I. Scegliere una Amazon Machine Image (AMI)
   I. Andiamo per Ubuntu 64bit
II. Scegliere il tipo di istanza
   I.  Prendiamo quella gratuita **t2.micro**
III. Dettagli della nuova istanza
IV. Aggiungere lo storage
V. Opzione Tag
VI. Configurare il Security Group
   I.  Creare nuova coppia chiave SSH e scaricala localmente
VII. Completare la creazione della nuova istanza

$ Creare un’istanza virtuale



$ Collegarsi all’istanza virtuale


Scaricare sul PC locale la chiave privata


Potrebbe essere necessario modificare i diritti della chiave privata

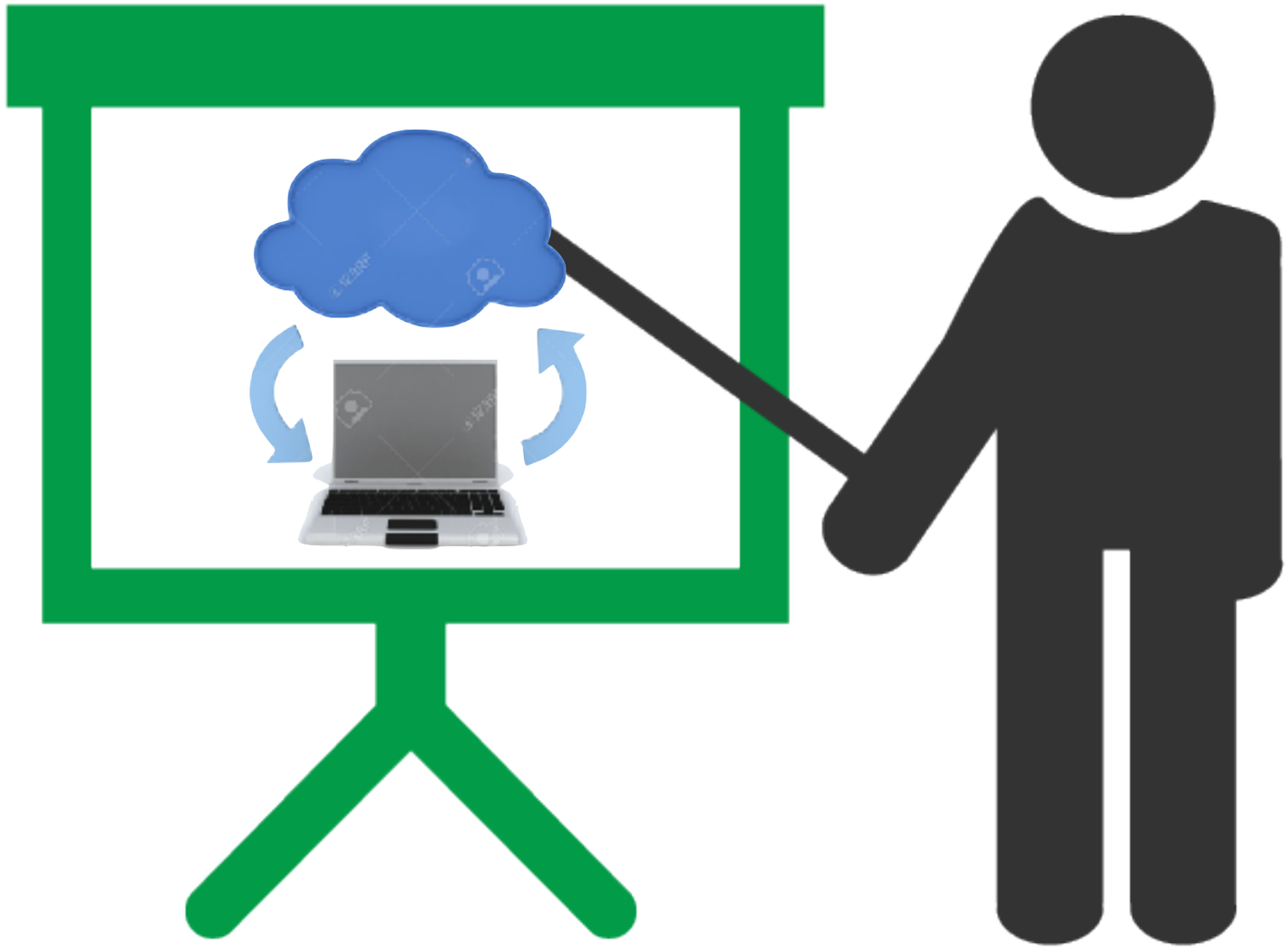
I. Aprire il terminale di Ubuntu sul PC locale

II. Spostarsi nella stessa directory della chiave privata

III. Collegarsi all’istanza usando SSH, esempio:

```
ssh -i "csm-ssh-key.pem" ubuntu@ec2-54-93-237-30.eu-
central-1.compute.amazonaws.com
```

$ Collegarsi all’istanza virtuale



$ Creare un Key Pair

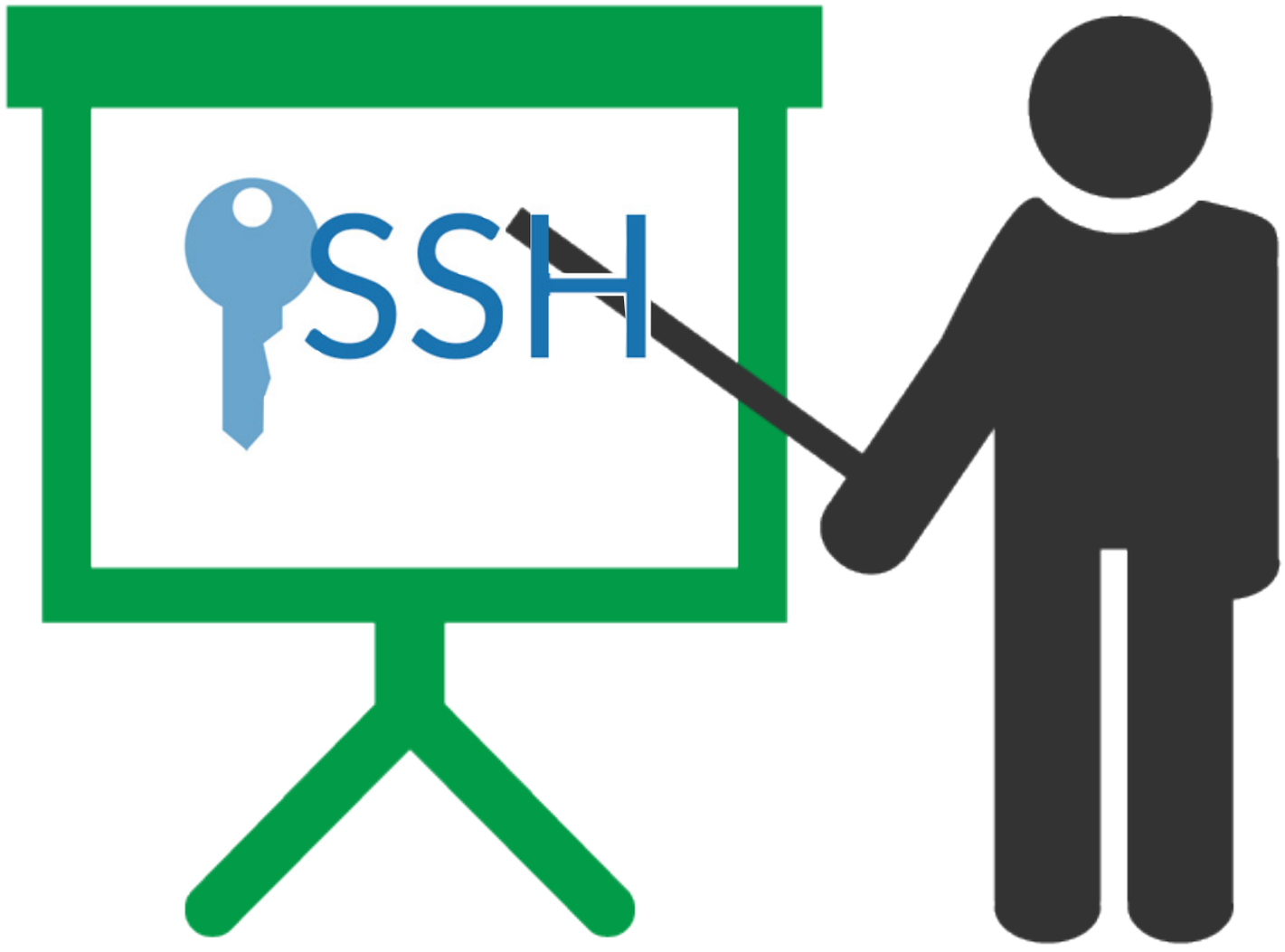
I. Cliccare su *Key Pairs* dalla console di EC2

II. Cliccare su *Create Key Pairs*

    I. Digitare il nome del nuovo *Key Pair*

III. Salvare la chiave privata in un posto sicuro del PC

$ Creare un Key Pair



$ Creare un Security Group

I. Cliccare su *Security Groups* dalla console di EC2

II. Cliccare su *Create Security Group*

    I. Digitare il Security group name

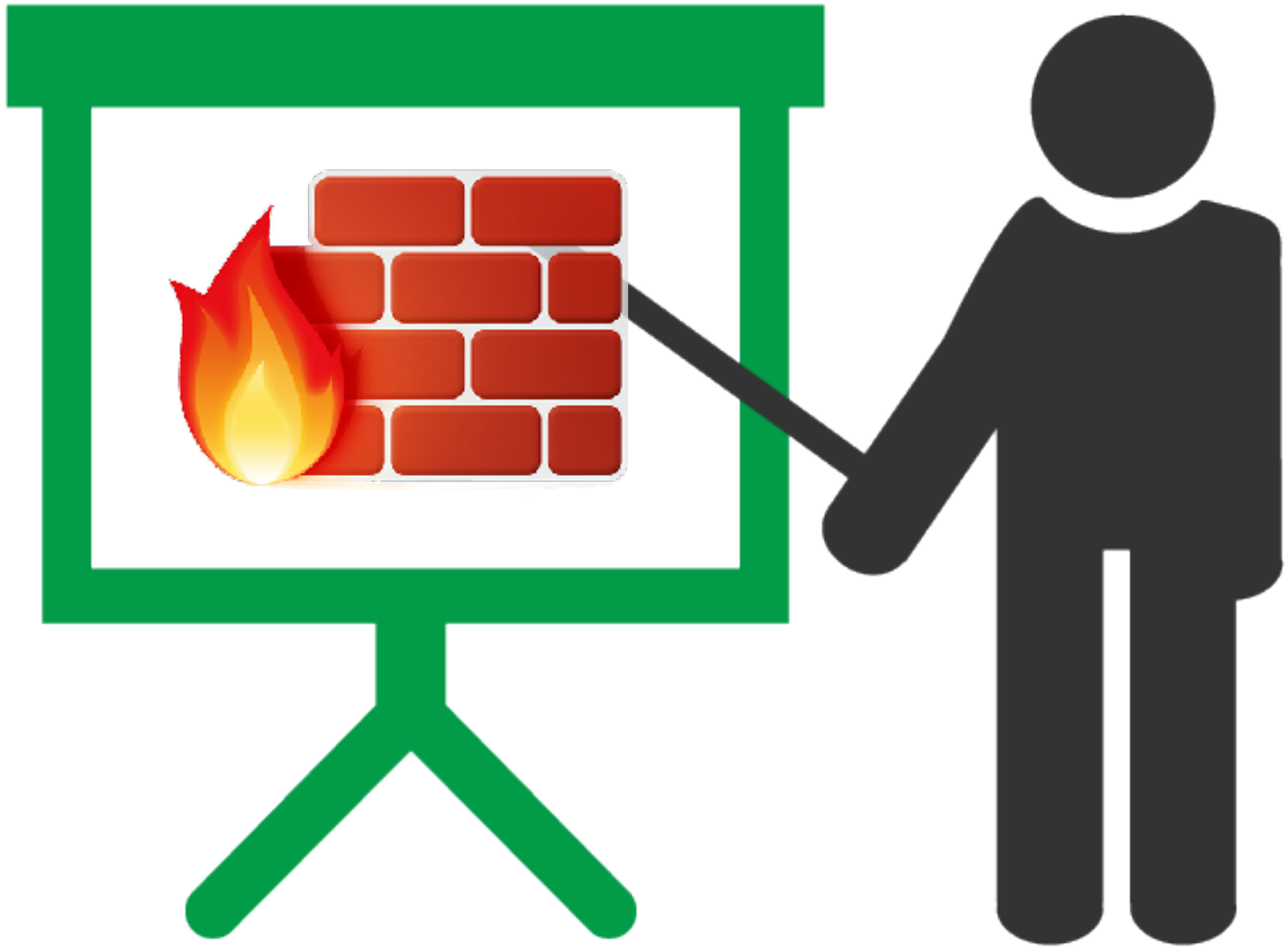
    II. Inserire una Descrizione

    III. Scegliere il VPC

III. Inserire le regole di *Inbound* and *Outbound*

IV. Cliccare su *Create*

$ Creare un Security Group



$ IpTables

- IpTables è un **firewall** a linea di comando;
- Controlla il traffico di ingresso, uscita e attraverso il PC attraverso tre “catene” di regole:
  - *Input chain;*
  - *Output chain;*
  - *Forward chain;*

- Le azioni da effettuare sul traffico sono comandate dalle regole scritte nelle catene;
- Di default IpTables non ha regole attive e le sue regole si cancellano ad ogni reboot se non sono rese permanenti

$ Configurare IpTables

Tutti i comandi vanno eseguiti con **sudo**

- Visualizzare tutte le regole impostate:
  - `iptables -L -v`
- Cancellare tutte le regole impostate:
  - `iptables -F`
- Bloccare tutto il traffico in ingresso:
  - `iptables -A INPUT -j DROP`
- Permettere i dati di ritorno di pacchetti inviati:
  - `iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT`
- Permettere traffico in ingresso da IP 146.48.56.83, protocollo TCP e porta 5432:
  - `iptables -A INPUT --source 146.48.56.83 -p tcp --dport 5432 -j ACCEPT`

$ Configurare IpTables

Tutti i comandi vanno eseguiti con **sudo**

- Permettere la loopback:
  - `iptables -I INPUT 1 -i lo -j ACCEPT`
- Permettere il protocollo **icmp**:
  - `iptables -A INPUT -p icmp --icmp-type 8 -s 0/0 -d `curl http://myip.dnsomatic.com` -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT`
  - `iptables -A OUTPUT -p icmp --icmp-type 0 -s `curl http://myip.dnsomatic.com` -d 0/0 -m state --state ESTABLISHED,RELATED -j ACCEPT`

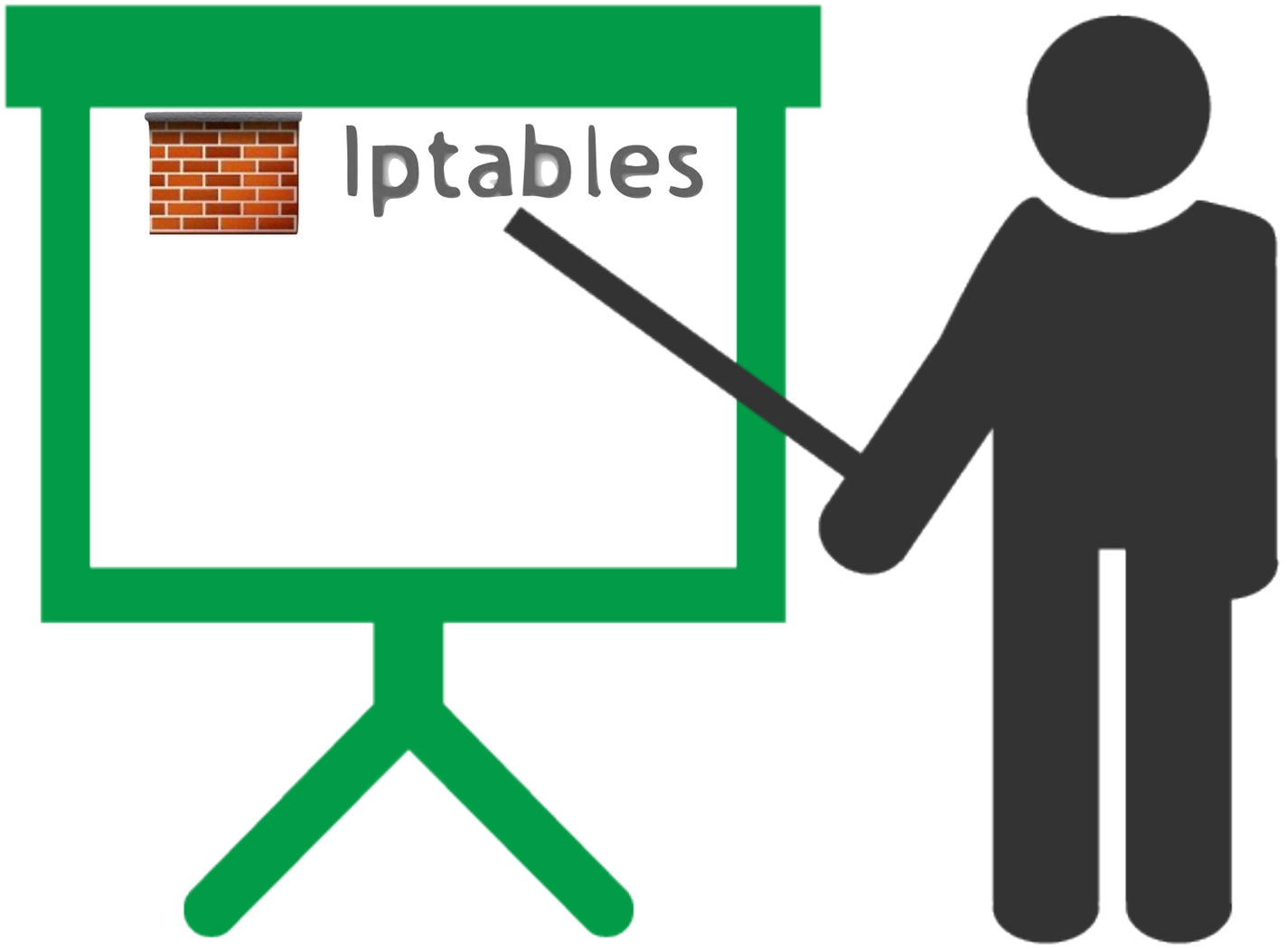
Provare **curl http://myip.dnsomatic.com** da terminale

$ Configurare IpTables

- Permettere traffico in ingresso da qualsiasi IP, protocollo TCP e porta 22 (**Quale servizio stiamo considerando?**):
    - `iptables -A INPUT --source 0.0.0.0/0 -p tcp --dport 22 -j ACCEPT`
- Mitigare **bruteforce attack**:
    - iptables -I INPUT -p tcp --dport 22 -i eth0 -m state --state NEW -m recent —set
    - iptables -I INPUT -p tcp --dport 22 -i eth0 -m state --state NEW -m recent --update --seconds 60 --hitcount 3 -j DROP
- Rendere le regole permanenti:
    - apt-get install iptables-persistent
    - e memorizzare le regole durante l’installazione

Tutti i comandi vanno eseguiti con **sudo**

$ Configurare IpTables



$ Sicurezza su SSH (auth.log)

- Il protocollo SSH memorizza le informazioni di connessioni sul file (Ubuntu):
  - /var/log/auth.log
- Estratto:

```
Sep  4 13:57:41 ip-192-168-2-230 sshd[25866]: Disconnected from 121.18.238.119 port 57695 [preauth]
Sep  4 13:59:12 ip-192-168-2-230 sshd[25868]: Received disconnect from 59.45.175.11 port 43583:11:  [preauth]
Sep  4 13:59:12 ip-192-168-2-230 sshd[25868]: Disconnected from 59.45.175.11 port 43583 [preauth]
Sep  4 14:30:12 ip-192-168-2-230 sshd[25897]: Accepted publickey for ubuntu from 129.12.113.122 port 62837 ssh2: RSA
```

Provare il comando **less /var/log/auth.log**
e osservarne il contenuto

- Problematiche
  - Tentativi di accesso
  - Dimensione Log
- Soluzione automatica: **denyhosts**

$ Sicurezza su SSH (auth.log)

- Problematiche:
  - Scoprire tentativi di accesso malevoli;
  - Dimensione Log;
- Soluzione interessante: **denyhosts**
- Guida per Ubuntu 16.04
  - https://www.cyberciti.biz/faq/how-to-install-denyhosts-intrusion-prevention-security-for-ssh-on-ubuntu/

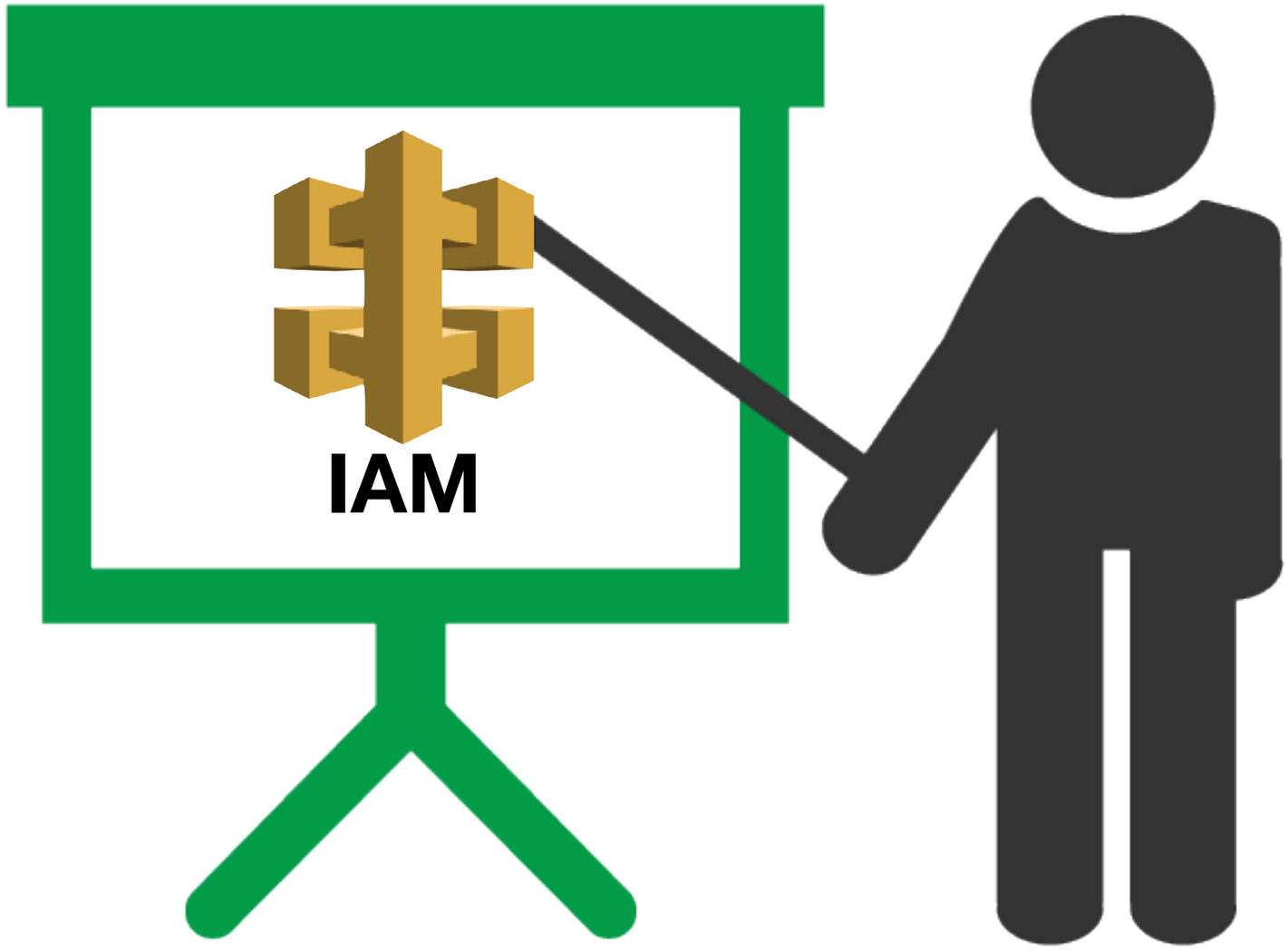
http://bit.ly/2j3HEkj

Osservare il contenuto di
sudo cat /etc/hosts.deny

$ Usare l'Identity and Access Management

I. Andare sulla "home" del pannello di AWS
II. Cliccare su IAM
III. Cliccare su Users
IV. Creare un nuovo utente cliccando su *Add user*
V. Digitare lo user name
    I. Es. testuser
VI. Selezionare il tipo di accesso AWS
    I. Programmatic access
    II. AWS Management Console access
VII. Creare un gruppo o selezionare un gruppo esistente
VIII. Finalizzare la creazione dell'utente

$ Usare l'Identity and Access Management



$ Creare una Virtual Private Cloud

I. Andare sulla “home” del pannello di AWS
II. Cliccare su VPC
III. Cliccare su start VPC Wizard
IV. Creare una nuova *VPC with a single Subnet*
V. Digitare la sottorete da creare
    I. Es. 192.168.0.0/16
VI. Digitare il nome della VPC
VII. Digitare la sottorete pubblica da creare
    I. Es. 192.168.1.0/24
VIII. Scegliere una Availability Zone
IX. Dare il nome alla sottorete pubblica
X. Creare la VPC

$ Creare una Virtual Private Cloud