

# CSA Italy:

## "Portabilità, interoperabilità e sicurezza applicativa nel cloud"



**OWASP Italy Day**

*"Web Security in a Mobile World"*

Rome - 23rd November 2012

# Cloud Security Alliance

Organizzazione internazionale no-profit

➤ Più di **+40,000** soci individuali, **+100** soci aziende, **+20** soci affiliati (associazioni), **+50** capitoli nel mondo

➤ Produrre **Guide (20 iniziative)** per un uso consapevole e sicuro di infrastrutture e servizi cloud computing



# CSA Italy



❑ **Associazione** associazione no-profit di diritto italiano

❑ **80 soci** regolarmente iscritti

❑ **Soci Affiliati:** 



❑ **Sponsor:** 



❑ **Collaborazioni:**   **OWASP** Italian Chapter  **Oracle** Community For Security



❑ **3 Gruppi di Ricerca** (+ risposta consultazione Garante)

❑ **+400 membri** nel LinkedIn group CSA Italy Chapter

# CSA Italy - Missione



- ✓ promuovere e sviluppare **temi di ricerca** sul cloud computing security, con particolare attenzione al mercato della **Piccola e Media Impresa (PMI) Italiana**;
- ✓ promuovere la **condivisione di conoscenza** del tema sia attraverso la partecipazione ad eventi/conferenze/seminari, accordi con associazioni professionali di settore e stampa specializzata;
- ✓ promuovere le **certificazioni professionali** gestite da CSA (CCSK);
- ✓ qualificarsi come interlocutore privilegiato nei **principali tavoli di discussione** sul cloud computing security.



# Ricerca 2012



## Gruppo di Lavoro “Traduzioni”

Coordinatore: *Yvette Agostini* – Sponsored by



## Gruppo di Lavoro “Portabilità, Interoperabilità e Sicurezza Applicativa”

Coordinatore: *Matteo Cavallini* – In collaboration with



OWASP  
Italian Chapter

Sponsored by



## Gruppo di Lavoro “Privacy & Legal in the Cloud”

Coordinatore: *Valerio Vertua* - Sponsored by



**Sottogruppo:** *Risposta alla consultazione pubblica di cui alle “Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali del 26 luglio (G.U. n. 183 7 agosto 2012)”*

# Ricerca 2012



Portabilità, interoperabilità  
e sicurezza applicativa



Novembre 2012



- **Coordinatore:** *Matteo Cavallini*
- **Autori/Contributori:** Matteo Cavallini, Alberto Manfredi, Yvette Agostini, Domenico Catalano, Mario Cola, Antonio Parata (*OWASP Italy*), Francesco Beatino, Eugenio De Santis
- **CSA-IT Staff** (Revisione grafica e produzione ebook)  
Paolo Foti

# I rischi: lock-in



## Portabilità, interoperabilità e sicurezza applicativa



Novembre 2012

 Allied Telesis  
Document Sponsor

## Portabilità e Interoperabilità

- Per gli utenti di servizi **SaaS** la problematica maggiore consiste nell'estrazione della banca dati del fornitore
- Per le applicazioni sviluppate su **PaaS**, invece, il rischio maggiore sorge quando il codice utilizza API non standard
- nei servizi **IaaS** le principali preoccupazioni sorgono nel caso in cui il formato con cui sono rappresentate le macchine virtuali non sia standard



# Gli obiettivi indicati



Portabilità, interoperabilità  
e sicurezza applicativa



Novembre 2012

Allied Telesis  
Document Sponsor

L'obiettivo è gestire le situazioni di:

- lock-in
- malfunzionamenti delle applicazioni a causa dell'**incompatibilità tra le piattaforme**, le applicazioni o i servizi erogati;
- reingegnerizzazione del processo e/o cambiamenti nel codice;
- cambiamenti inattesi dei dati causati dalla carenza di "data format" portabili ed interoperabili;
- **modifiche sostanziali alle applicazioni** e/o software di gestione;
- manifestazione di **lacune di sicurezza e/o vulnerabilità** latenti causate da differenze nelle politiche di sicurezza, nella gestione delle chiavi o nella protezione dei dati, da parte di differenti fornitori cloud.



# Processo di gestione



Portabilità, interoperabilità  
e sicurezza applicativa



Novembre 2012



## Secure Software Development Life Cycle

- Strategia di Governance
- Implementazione, che racchiude anche tutti i metodi e criteri adottati per la realizzazione di un'architettura software sicura (comprese le attività di Secure Code Review" e di "Threat Modeling")
- Collaudi di Sicurezza
- Contromisure e continuità d'esercizio" che prevede le attività di "Code Mitigation" e di "Progettazione difensiva"

# Prossime iniziative

- ✓ Nel 2013 CSA Italy avvierà una ricerca finalizzata alla realizzazione di un documento di indirizzo e linee guida per l'applicazione dei modelli SSDLC e SDL nelle attuali soluzioni Cloud ed ai relativi modelli di deployment.
- ✓ Questo documento costituirà un punto di riferimento per i CSC per la determinazione delle responsabilità in tema di sicurezza delle applicazioni software nei vari modelli di cloud.
- ✓ L'obiettivo finale è di produrre un documento che comprenda degli schemi di allocazione delle relative responsabilità ai vari attori coinvolti nello specifico delle varie fasi e attività dello sviluppo applicativo.

# GRAZIE



**Matteo Cavallini**  
*Vice-President*

***[www.cloudsecurityalliance.it](http://www.cloudsecurityalliance.it)***  
***[cloudsecurityalliance.org](http://cloudsecurityalliance.org)***

***[matteo.cavallini@csaitaly.it](mailto:matteo.cavallini@csaitaly.it)***  
***Twitter account: @nientenomi***