



accenture


High performance. Delivered.

The approach to the application security in the cloud space

Manuel Allara

CISSP CSSLP

Roma – 28 Ottobre 2010



>> Introduzione

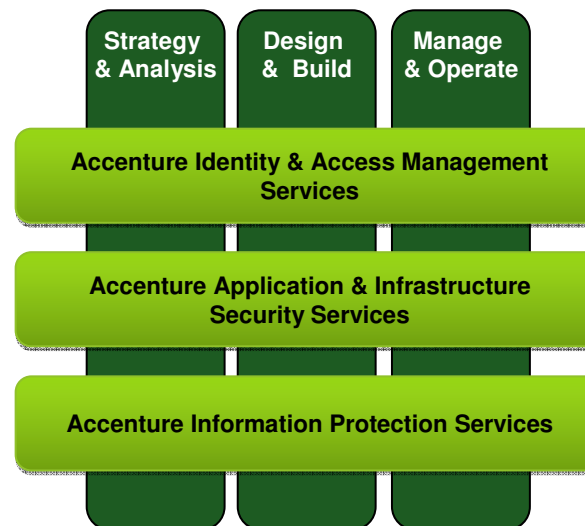
Accenture Security Service Line

La Security Service Line di Accenture supporta i clienti sulle tematiche di sicurezza informatica grazie ad un team di 1800 professionisti nel mondo

Security Service Line

- ❑ **Team di 1800 professionisti nel mondo**
 - > 100 in Italia
 - > 180 in IDC (India Delivery Center)
- ❑ **Personale certificato con i principali standard di mercato**
 - CISSP, CISA, ISO27001, SANS, BS25999, etc
 - CSSLP (Certified Secure Software Lifecycle Professional)
- ❑ **Esperienze di progetto su tutte le principali tematiche dell'IT Security**
- ❑ **Competenze di prodotto diversificate sui prodotti leader di mercato e su altri tool di application security**
- ❑ **Delivery Center per gestione in outsourcing di attività di Security**
 - Italia, India, Praga
- ❑ **Asset**
 - Metodologie, framework e strumenti sviluppati dai team di Accenture

Offerings




Principali Alliance



Principali Clienti

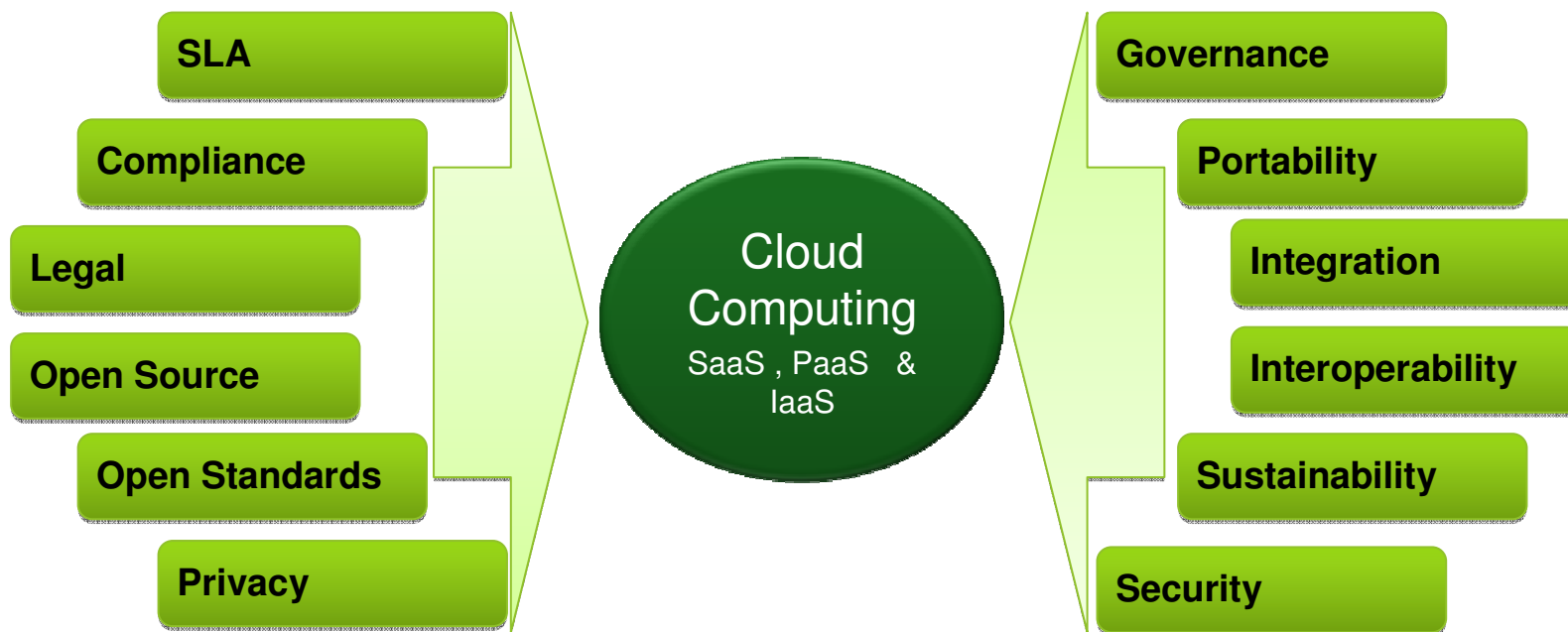




>> Contesto

Cloud Space: Punti di attenzione

L'adozione di un modello cloud-based richiede attente considerazioni tecnologiche e operative

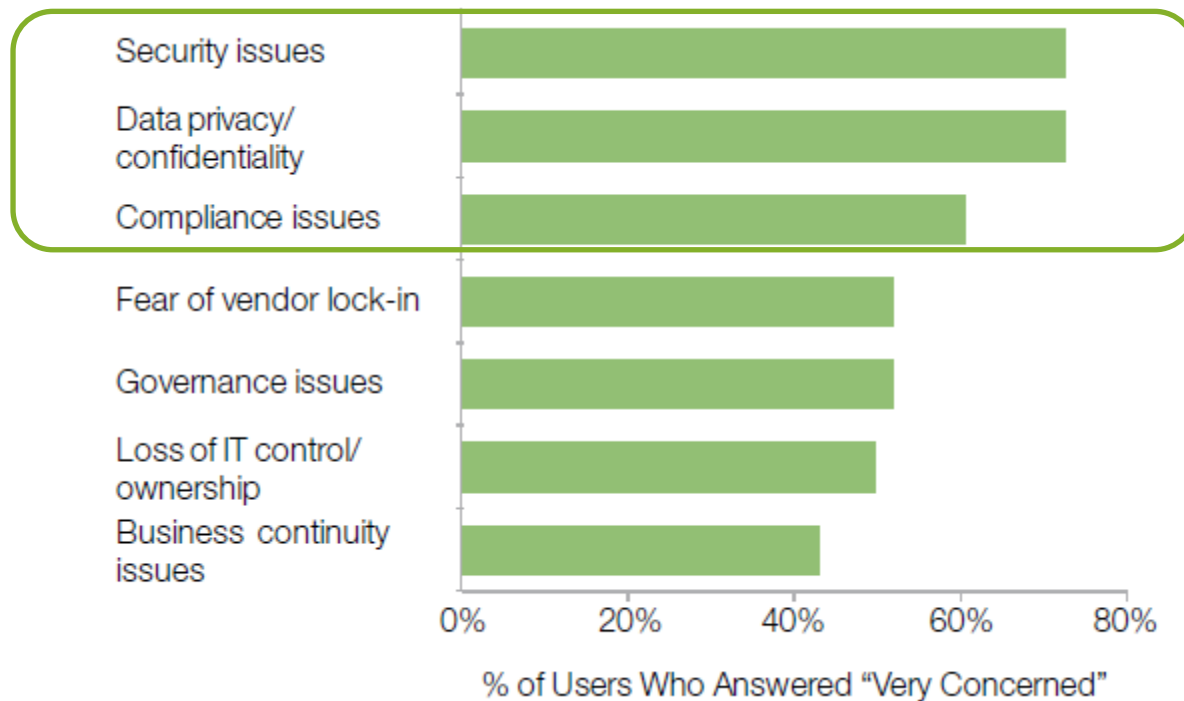




>> Contesto

Percezione della sicurezza legata al cloud

Quali sono le principali preoccupazioni quando si acquistano servizi “cloud-based”?

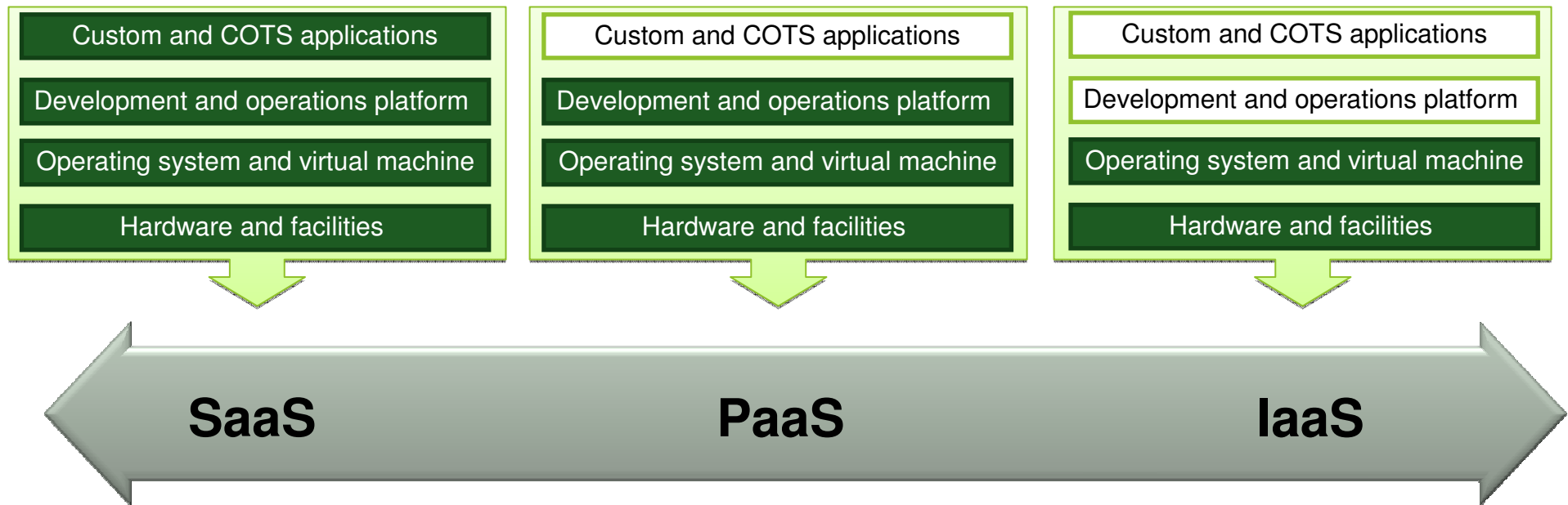


*Cloud Computing Survey 2009,
World Economic Forum and
Accenture*



>>Application Security nei modelli di servizi cloud-based

Modelli di erogazione di servizi cloud e gestione della sicurezza applicativa



Tipicamente il cliente controlla poco o nulla delle applicazioni fornite. Il provider di SaaS è il maggiore responsabile della sicurezza applicativa

Un PaaS cloud provider offre un ambiente per il design, sviluppo, test, deploy, e supporto delle applicazioni custom. L'application security in questo caso riguarda fundamentalmente la sicurezza della piattaforma stessa (runtime engine) e la sicurezza delle applicazioni deployate sulla piattaforma PaaS

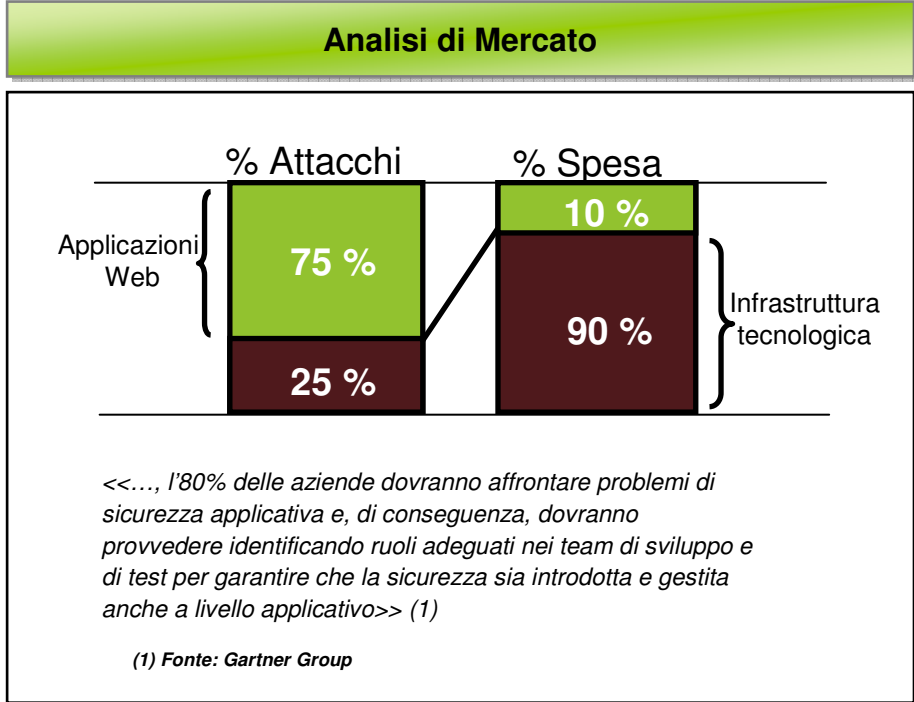
Un IaaS cloud provider considera l'applicazione del cliente come una black box . L'intero stack applicazione e piattaforma di run time è gestito dal cliente così come la sicurezza applicativa



>>Application Security nei modelli di servizi cloud-based

Analisi di Mercato – Rischi legati alle vulnerabilità applicative

Dall'analisi del mercato emerge un forte **squilibrio** fra **target degli attacchi** e **gli investimenti delle aziende a protezione degli stessi**.



- Rischi Principali**
- **Frodi interne ed esterne**, accesso e/o modifica di dati riservati da personale dipendente, terze parti, clienti, attacchi da rete internet, etc
 - **Interruzione del business** blocco dei servizi, blocco dei sistemi, cancellazione dei dati, etc
 - **Responsabilità legali – penali** (utilizzo di facilities e sistemi aziendali per frodi e azioni illecite verso terzi, distribuzione di malware a terze parti e clienti, etc)
 - **Responsabilità legali – sanzioni** (privacy, azioni di rivalsa, etc)
 - **Perdita di immagine** (divulgazione sui media di avvenuti attacchi e di vulnerabilità dei servizi)
- la Repubblica.it** Tecnologia&Scienze

ROMA - C'è un buco nel sistema di sicurezza di eBay. Un buco che si apre e che si chiude di continuo, come la porta automatica di un grande magazzino. E che permette a qualunque hacker minimamente capace di entrare in possesso delle informazioni personali riservate dei clienti. E di derubarli. Noi questo buco lo abbiamo individuato, lo abbiamo aperto e poi ci siamo entrati dentro (il video si può vedere sul sito di RepubblicaTv).

Dimostrando, così, quanto sia semplice rubare i dati personali e bancari degli utenti eBay che partecipavano a una determinata asta. Un'asta come tante, usata però come esca. Con l'aiuto di un hacker abbiamo sfruttato quella che tecnicamente si chiama vulnerabilità "cross-site scripting". L'operazione non è così complessa come sembra.

>>Application Security nei modelli di servizi cloud-based Trend su Application Security

La maggior parte delle aziende sta **affrontando problemi di sicurezza applicativa** e, di conseguenza, deve provvedere ad identificare **ruoli adeguati nei team di sviluppo e di test** per garantire che la sicurezza sia introdotta e gestita anche a livello applicativo.

❑ Driver Tecnologici

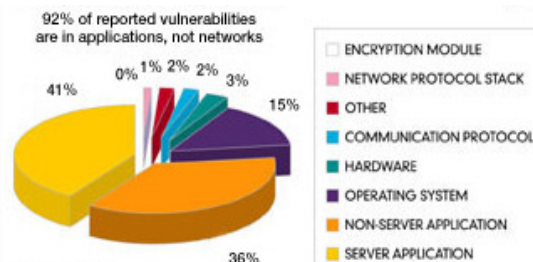
- Aumento della complessità delle architetture applicative e perdita di un perimetro che divide l'area trusted da quella untrusted
- Alti costi delle eventuali remediation del software prodotto
- Aumento delle minacce focalizzate sugli applicativi e conseguente aumento del rischio

❑ Driver di Business

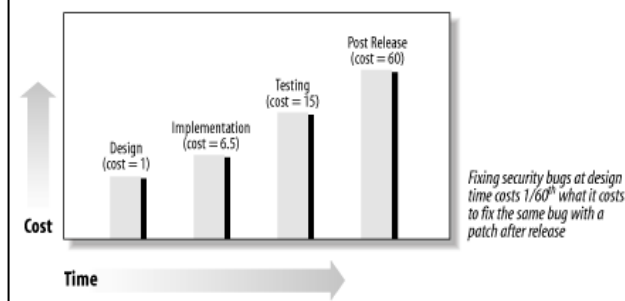
- Rischio di frodi
- Rischio di perdita di informazioni riservate
- Rischio di perdita di reputazione in caso di compromissione di applicativi contenenti dati riservati

❑ Driver Normativi

- Conformità PCI e diversi provvedimenti del Garante



Il 92% delle vulnerabilità identificate sono nelle applicazioni, non nella rete (fonte NIST)

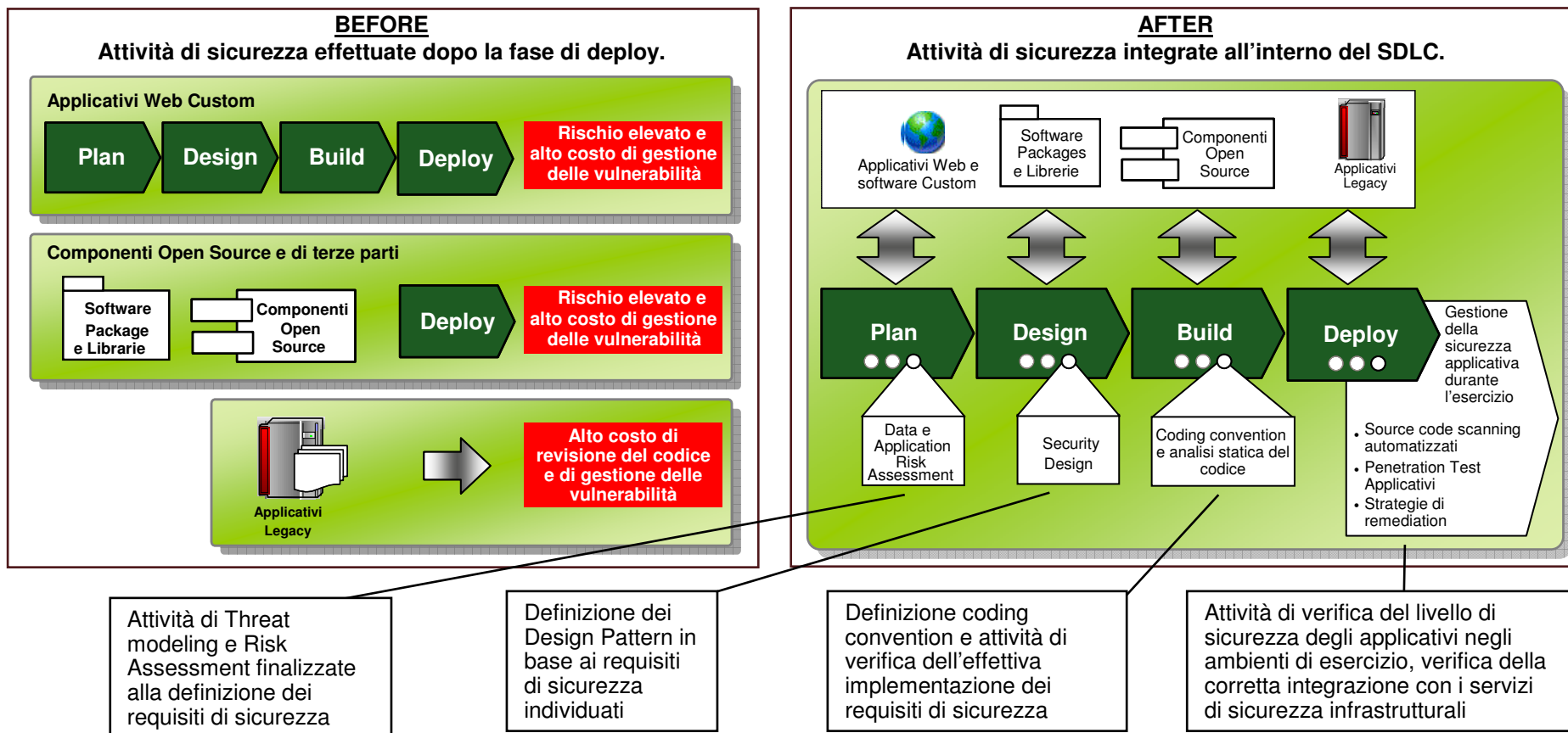


Il costo di remediation degli errori incrementa in base alla fase in cui è individuato (fonte NIST)



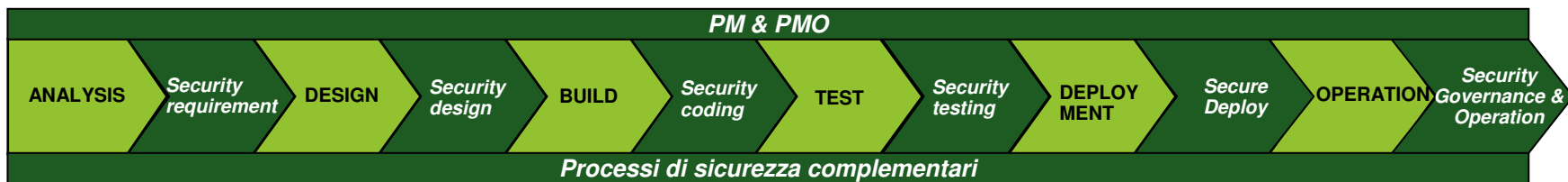
>>Application Security nei modelli di servizi cloud-based

Enterprise Application Security – Secure SDLC



>> Approccio Accenture

Introduzione di attività di application security nel ciclo di vita del SW



Insieme di attività volte alla definizione dei requisiti di sicurezza da implementare nelle fasi successive



Sulla base dei requisiti precedentemente definiti e delle best practice di sicurezza vengono definiti i design pattern di riferimento, threat modeling e design review



Attività volte a definire le coding convention di sicurezza per i linguaggi di programmazione utilizzati al fine di guidare il programmatore nella stesura sicura del software



Attività e strumenti volti all'individuazione di problematiche relative alla security: checklist, analisi statica del codice, security assessment, Dynamic Analysis, security test cases



Verifica della corretta integrazione dei servizi di sicurezza dell'ambiente di produzione con gli applicativi, della presenza di eventuali vulnerabilità e remediation delle stesse




Definizione di una strategia di sicurezza applicativa, di ruoli e responsabilità, di processi di gestione, di policy, di metriche, di KPI e di un modello di rating



Insieme di processi di sicurezza complementari al SDLC che mirano a rendere sicuri gli ambienti



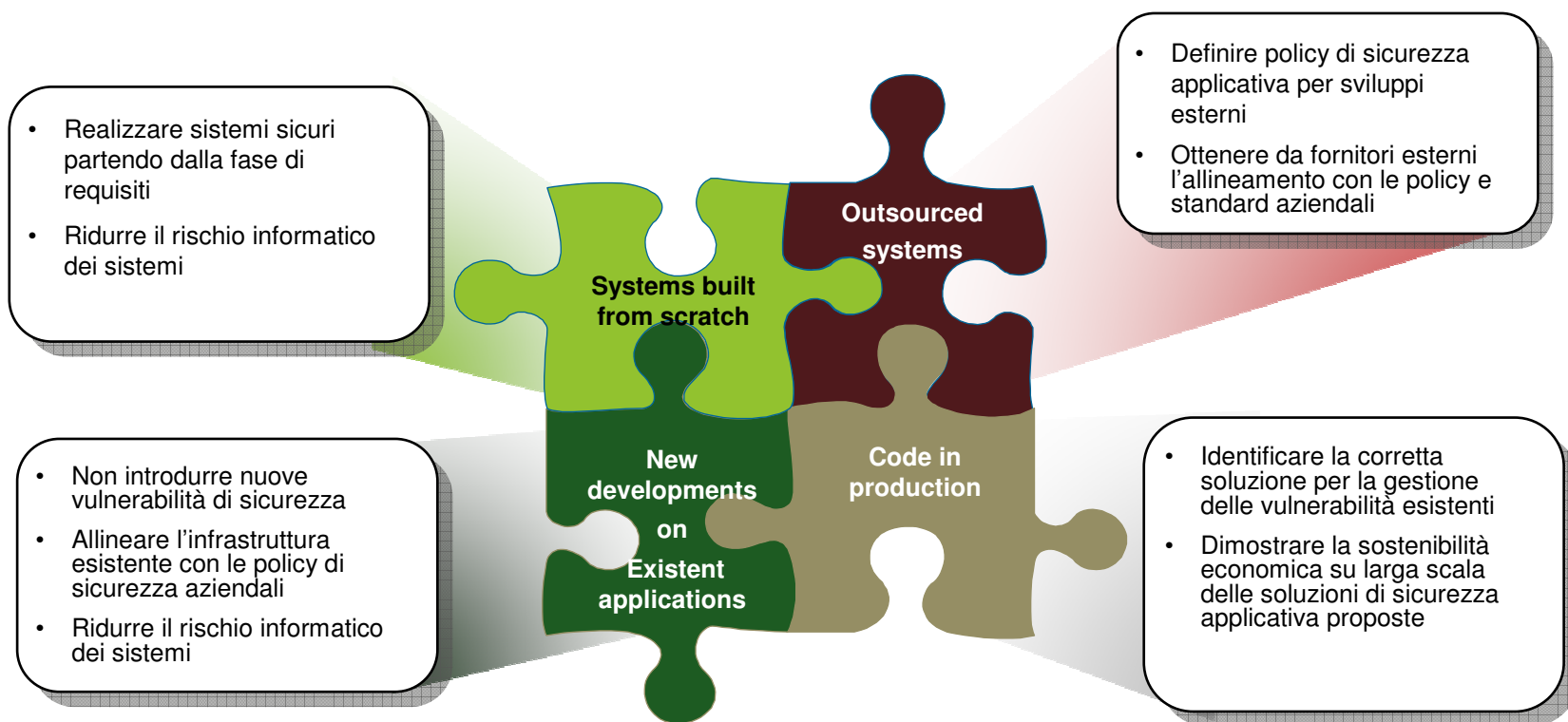
Attività di PM e PMO tra cui coordinamento e gestione risorse e progetto interno, SAL, coordinamento e gestione vendor

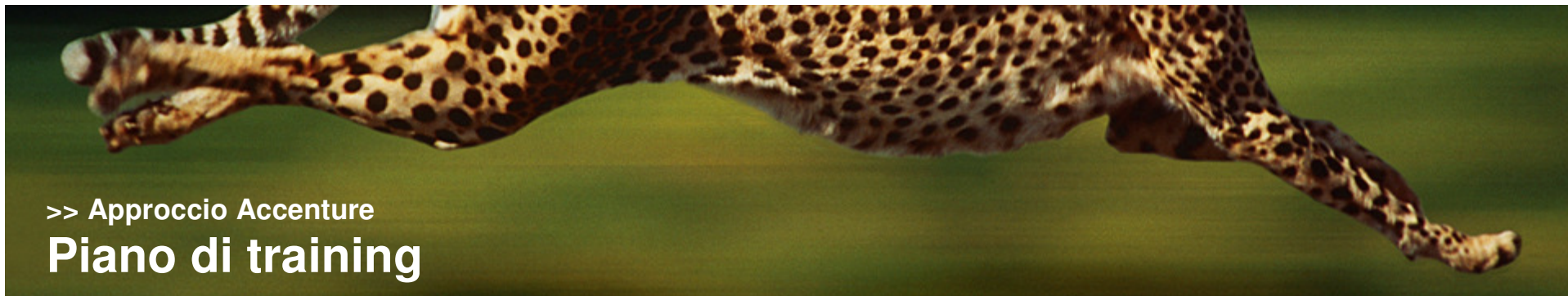


>> Approccio Accenture

Le dimensioni della realtà aziendale

La sicurezza dell' **SDLC** coinvolge potenzialmente l'intero parco applicativo comprendendo applicazioni nuove o esistenti, sviluppi interni o affidati a fornitori esterni, infrastrutture interne o esterne, applicazioni custom o package.

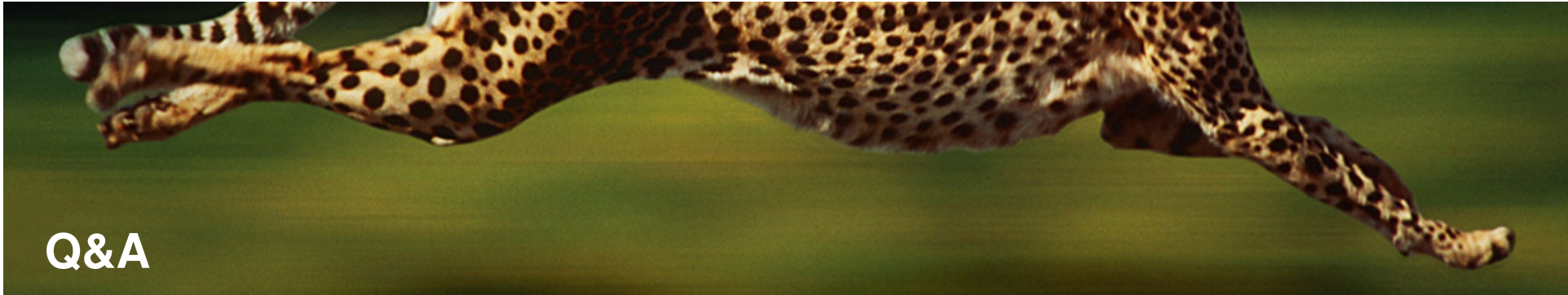




>> Approccio Accenture
Piano di training

Una delle componenti fondamentali di un progetto di Secure SDLC è il **piano di formazione** di tutti gli attori coinvolti nel ciclo di vita del software. La formazione dovrà avere **uno scopo ed un livello di dettaglio adeguato** al ruolo delle persone.

Tipologia	Descrizione	Argomenti	Target
Security Awareness	Formazione generica finalizzata alla comprensione dei principali concetti di sicurezza.	<ul style="list-style-type: none"> • Confidenzialità, Integrità, Disponibilità • Autenticazione, Autorizzazione, Accounting • Classificazione delle Informazioni e Data Privacy • Overview su Leggi, Standard e Best Practices • Incidenti di sicurezza 	Tutti i dipendenti
Security Technical Awareness	Formazione finalizzata all'individuazione dei requisiti tecnologici minimi necessari a garantire le proprietà di sicurezza degli applicativi e alla progettazione delle specifiche tecniche nel rispetto dei requisiti.	<ul style="list-style-type: none"> • Minacce, vulnerabilità, livello di rischio • Problematiche applicative • Standard di sicurezza (PCI, ISO 27001) • Leggi e decreti (D. Lgs. n.196/2003) 	Tutti i dipendenti IT
Secure Architecture Design	Formazione finalizzata a definire architetture applicative per garantire un adeguato livello di sicurezza.	<ul style="list-style-type: none"> • Secure Design • Threat modeling – attack tree • Tecnologie/architetture di sicurezza specifiche del framework (ad esempio Java Security) 	Security Designer Resp. Sviluppo
Secure Coding	Formazione indirizzata agli sviluppatori al fine di produrre codice sicuro.	<ul style="list-style-type: none"> • Vulnerabilità Applicative • Secure Programming • Strumenti di Static Code Analyzer 	Sviluppatori Resp. Sviluppo
Secure Audit	Formazione per la realizzazione delle verifiche al fine di valutare il livello di sicurezza degli applicativi.	<ul style="list-style-type: none"> • Vulnerabilità applicative • Secure Testing • Remediation 	Security Auditor



Q&A



	Manuel Allara
	Technology - Security
	Accenture Viale del Tintoretto 200 Rome – Italy
	0039-334-6418892 manuel.allara@accenture.com