Application Security Governance

28 ottobre 2010

Francesco Baldi

Security & Risk Management
Practice Principal

AGENDA

- Problematiche di sicurezza applicativa
- Modello di riferimento
- Processo di sicurezza applicativa
- HP Application Security Tracking and Audit Tool
- Benefici

PROBLEMATICHE DI SICUREZZA APPLICATIVA

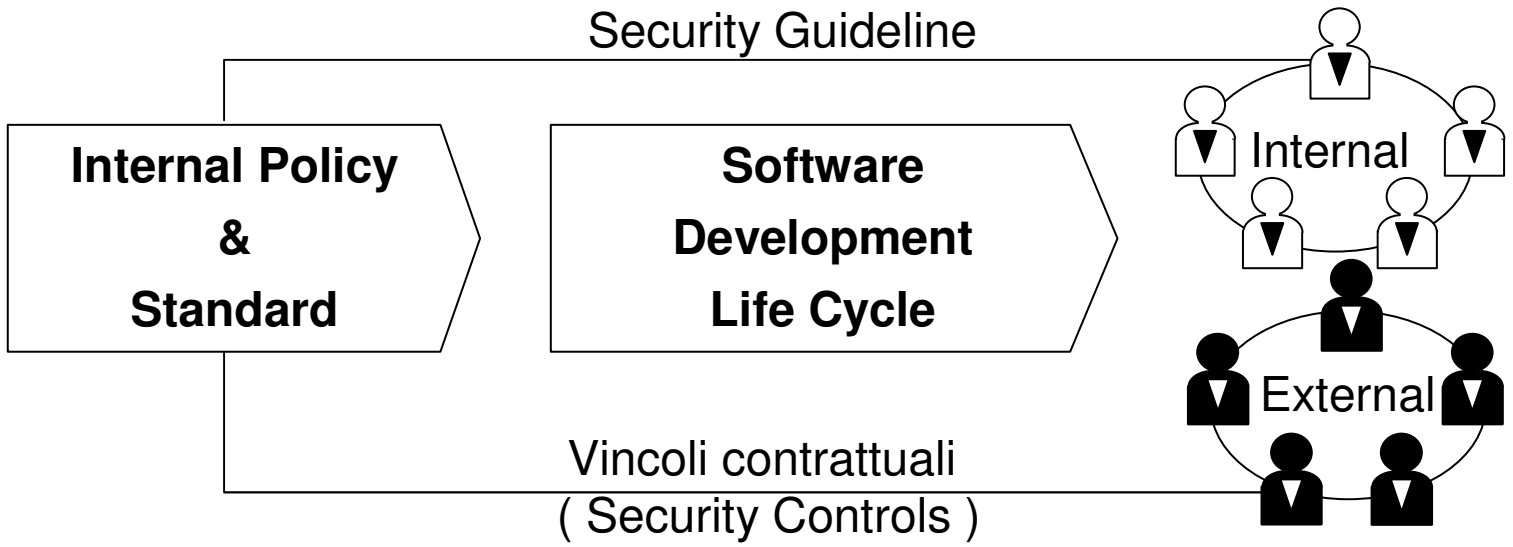
- Mancanza di requisiti di sicurezza durante la fase di progettazione, sviluppo e di revisione delle applicazioni. In genere non vengono opportunamante considerati i requisiti di sicurezza. Questo ha impatto sia in termini di costi di gestione complessiva sia in termini di definizione delle priorita' di sviluppo. La percezione comune e' quella di affrontare le problematiche di sicurezza applicativa utilizzando prodotti e procedure specifiche per la sicurezza. Cio' rafforza la concezione che i requisiti di sicurezza sono "**out-of-scope**" rispetto al problema della progettazione e implementazione.

- Difetti di implementazione e di progettazione, conosciuti e sconosciuti, incrementano in modo significativo il rischio di utlizzo improprio delle applicazioni. I relativi "security bulletins" sono solo l'evidenza di un problema molto piu grave. Per esperienza interna HP le vulnerabilita' riscontrate con **metodi tradizionali** sono circa il 5% delle vulnerabilita' totali.

- Le legislazioni e normative vigenti (Basilea II, PCI, Privacy,…) richiedono l'aumento del livello di attenzione sulle problematiche della sicurezza. Attualmente il tentativo di rispondere adeguatamente a tali requisiti ha impatto su tutto il **ciclo di vita** della applicazioni sia in termini di definizione dei requisiti di sicurezza, di sviluppo e di test.

APPLICATION SECURITY GOVERNANCE

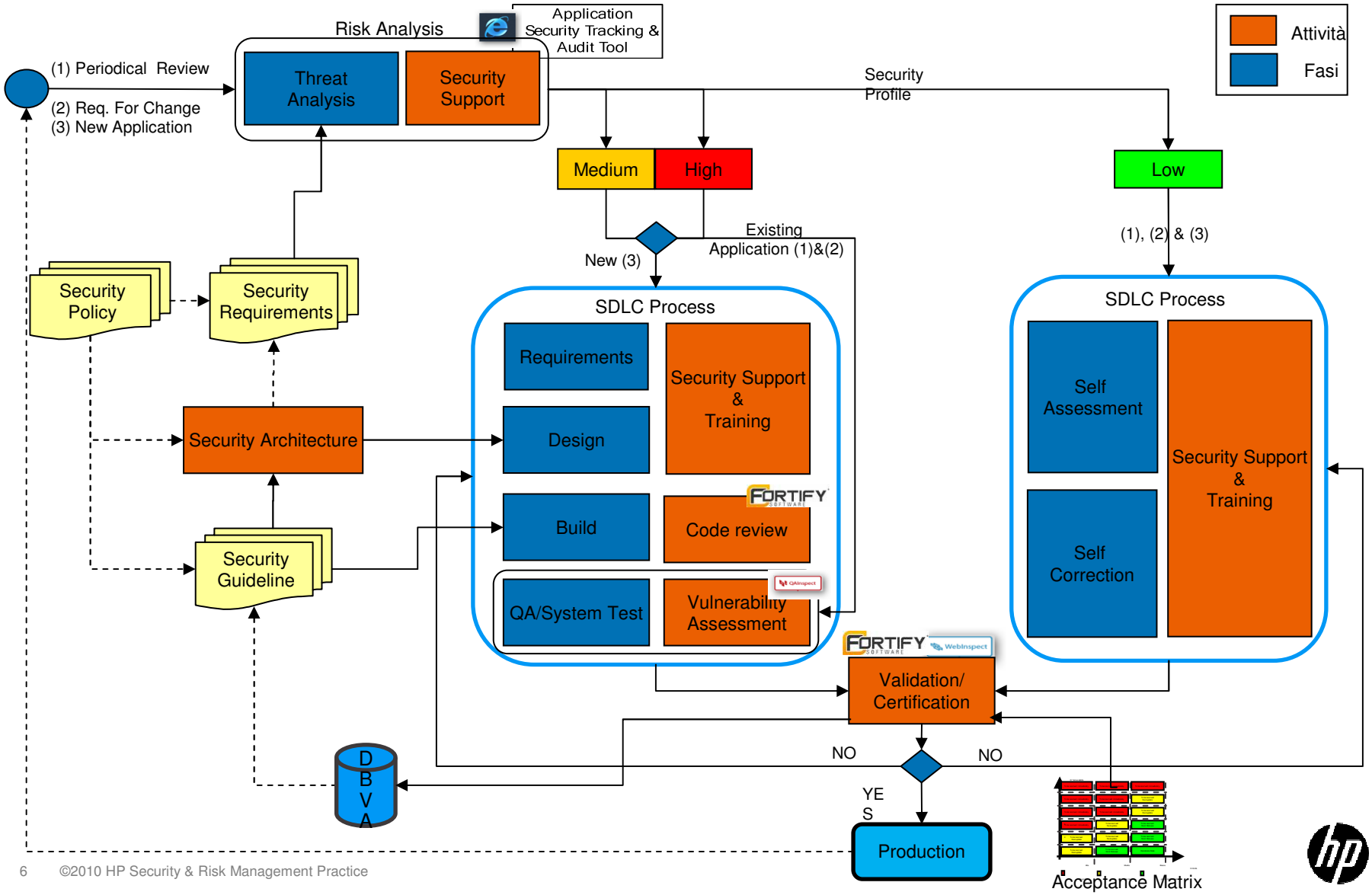
Il processo di **Application Security Governance** ha lo scopo di guidare, coordinare e suggerire le azioni necessarie a garantire la la gestione della sicurezza applicativa.



OBIETTIVI

- Consentire la valutazione sistematica ed il controllo del livello di sicurezza delle applicazioni.
- Garantire di conformità a standard, normative e Best Practice
- Definire una metodologia di analisi atta a supportare il processo di sicurezza applicativa dellle applicazioni, all'interno del più ampio processo di gestione del ciclo di vita del software o di ognuna delle sue fasi (Design, Build, Acceptance testing, Roll-out).
- Validare/Certificare le applicazioni che abbiamo il livello di sicurezza definito durante la fase di accettazione
- Introduzione di metriche di valutazione dei fornitori interni ed esterni
- Gestione del rischio
- Facilitare la formazione del personale sulle tematiche di sicurezza applicativa.
- Storicizzazione dei risultati allo scopo di monitorare le evoluzioni e gestire il rischio associat
- Introduzione chekpoint di sicurezza nel processo di gestione del ciclo di vita del software (SDLC) (Design, Build, Acceptance testing, Roll-out).

MODELLO DI RIFERIMENTO



ASTA (**A**PPLICATION **S**ECURITY **T**RACKING AND **A**UDIT TOOL)

ASTA è un tool web disegnato e sviluppato internamente ad HP per assistere lo sviluppo e la creazione di applicazioni garantendo il livello di sicurezza definito.

L'adozione di tale strumento contribuisce ad aumentare significativamente il livello di consapevolezza della sicurezza, di conformità alle policy e alle normative, tracciandone lo stato di conformità e storicizzando i risultati.

Componenti:

- **Threat Analysis,**
- **Application Security Review**
- **On-demand Web Application Security Scan**

ASTA THREAT ANALYSIS

ASTA Threat Analysis:

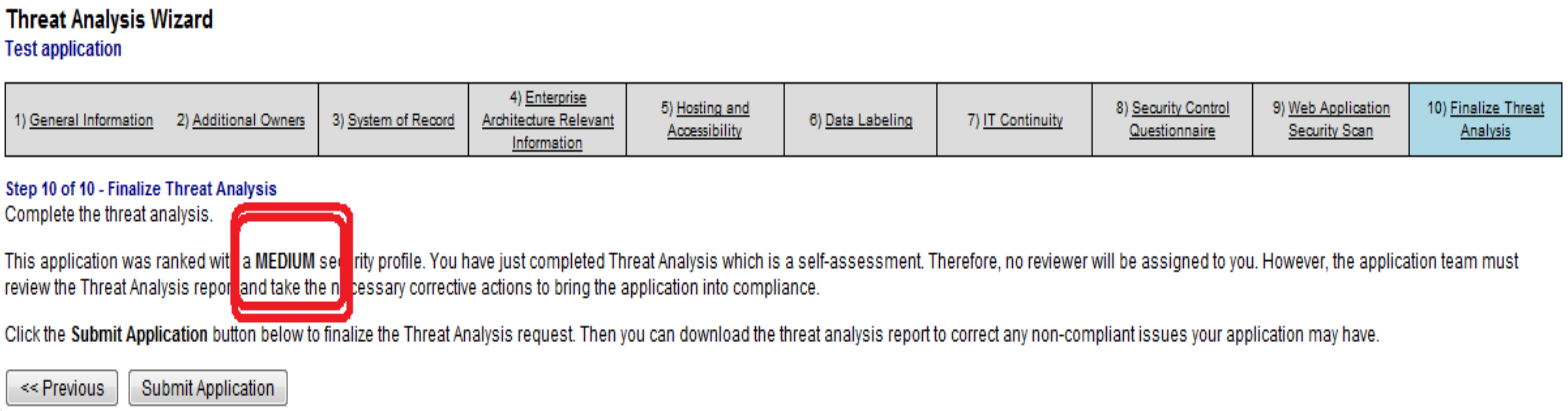
E' utilizzata in fase di design di un'applicazione per condurre un'analisi delle minacce ("self-help risk analysis")

è uno strumento di analisi dei rischi basato su un semplice sistema esperto che fornisce consigli di sicurezza a progettisti e architetti relativamente a requisiti di sicurezza dettati dalle policy.

•Collezione le informazioni specifiche dell'applicazione

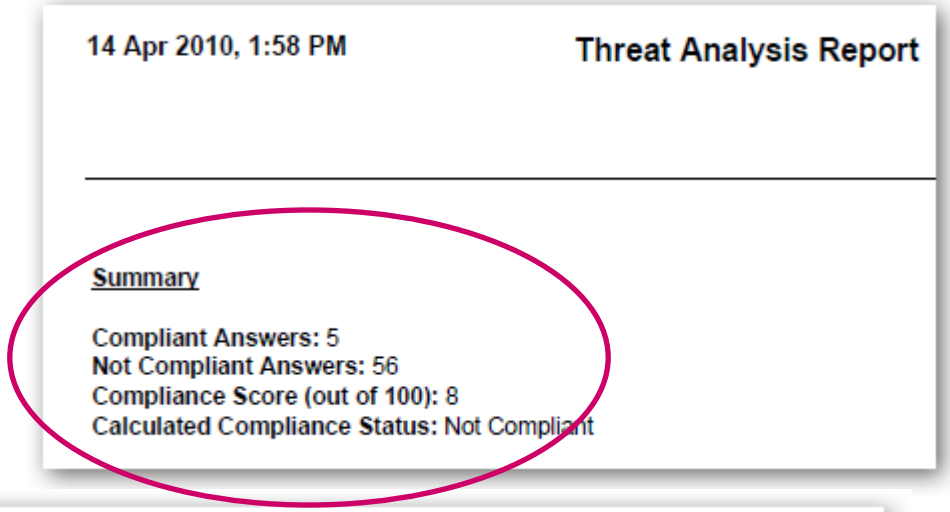
•Assegna le priorità all'applicazione, relativamente ai dati trattatti, al valore monetario dell'applicazione, ...

•Individua i controlli di sicurezza previsti,....



ES: ASTA (THREAT ANALYSIS REPORT)

Al termine dell'analisi viene generato un report con il livello di rischio dell'applicazione, con l'elenco delle policy di sicurezza non ripettate ed i consigli per rendere l'applicazione policy compliance.



14 Apr 2010, 1:58 PM

Threat Analysis Report

Summary

Compliant Answers: 5
Not Compliant Answers: 56
Compliance Score (out of 100): 8
Calculated Compliance Status: Not Compliant

Based on the information you provided, ASTA has determined you have 56 issues that are not in compliance with HP Security Policies and Standards, and industry best practices.

1) Authentication Compliance - ASTA has determined you are required to use class A authentication at the network boundary. See the table of required authentication. This means the gateway or proxy must use HP-IT issued ActivCard or HP-IT issued SecurID authentication. Is your application in compliance with class A authentication? Notes: if the external access to the application is limited to HP employees or HP Contingent Workers who are using MSRA, the application is compliant since MSRA uses class A authentication.
Answer: No - NOT COMPLIANT
The gateway or proxy must use HP-IT issued ActivCard or HP-IT issued SecurID authentication.
Policy / Standard - Authentication Policy

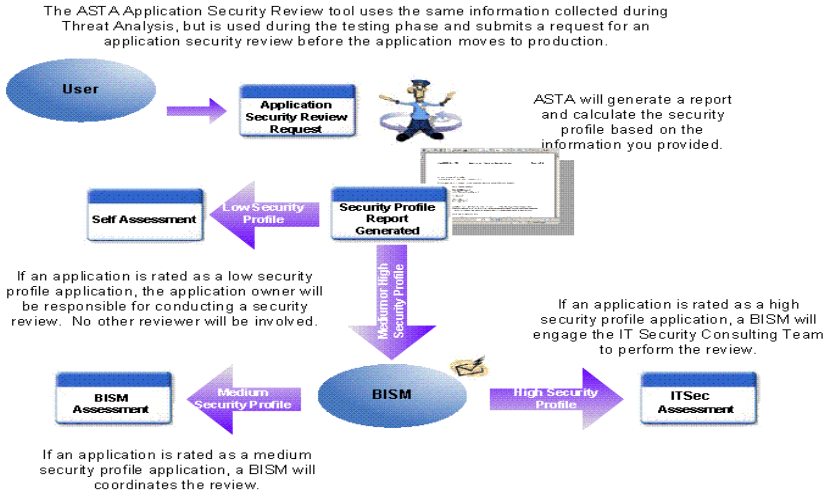
This report is compiled from a subset of the full security policy base to assist in the design of secure applications. Addressing all the non-compliant issues in this report does not guarantee the mitigation of all security vulnerabilities for your application. However, it provides a solid basis for avoiding common mistakes and mitigating high risk threats.

Your application has a **HIGH** security profile.

ASTA APPLICATION SECURITY REVIEW/ON DEMAND

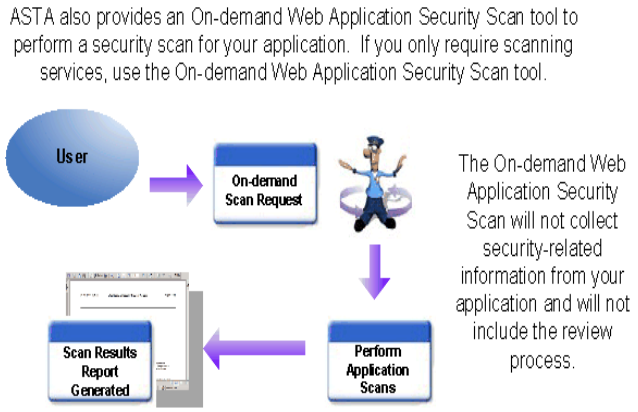
ASTA Application Security Review è uno strumento utilizzato durante la fase di test per permettere una revisione di sicurezza dell'applicazione prima dello spostamento in produzione.
In base al livello di rischio assegnato all'applicazione, prevede tre approcci diversi:

- *Security profile Basso* → self assessment
- *Security profile Medio* → ingaggio di una risorsa BISM
- *Security profile Alto*: → ingaggio del gruppo IT Security



ASTA On Demand e' utilizzato durante la fase di costruzione e/o test.

Fornisce un servizio per il controllo delle vulnerabilità dell'applicazione.



CONCLUSIONI

SHIFTING THE FOCUS FROM CODE TO ARCHITECTURE

"Test Security In" Approach

- Applications developed with high rate of latent security vulnerabilities
- Thousands of vulnerabilities reported per year (NVD); many more undetected
- Catch vulnerabilities with code scanners, security code analysis, penetration testing, etc.

"Design Security In"

- Analyze security requirements gaps
- Analyze architectural security resiliency to coding errors
- Avoid introduction of many vulnerabilities
- Prioritize security testing efforts

BENEFICI
CASE STUDY (*)

Reduce Cost

- 50% riduzione costi di attività esterne di security assessment (pen test)
- 60% riduzione COF (Cost Of Fixing) a regime
- 40% riduzione costi legati ad attività di audit e conformità (PCI, Garante Privacy)

Mitigate Risk

- Rduzione rischi legati alla diminuizione del'interruzione dei servizi verso i clienti
- Attuazione del processo di gestione del rischio
- Riduzione del numero di defect e del tempo per completare gli auditing.

* Based on ROI study on an HP client experience

BACK