June 6, 2017

Agile nei servizi di Cyber Security

Fabrizio Tocci
Simone Onofri

DXC.technology

Simone Onofri

Cyber Defense Lead per l’Europa Sud @ DXC

Fabrizio Tocci

PM Lead per i Security Advisory Services per l’Europa Sud @ DXC

Thrive on change

DXC.technology

DXC Technology è un’azienda leader per servizi IT end-to-end. Guidiamo i clienti nelle loro trasformazioni **digitali**, **moltiplicando** le loro capability, aiutandoli a sfruttare la potenza dell’innovazione e a capitalizzare sul cambiamento.

CSC e HPE Enterprise Services hanno innovato clienti per più di 60 anni

Insieme, lavoriamo per **circa 6000 clienti pubblici e privati in più di 70 paesi**

I nostri clienti ottengono benefici dall’**indipendenza tecnologica, talenti in tutto il mondo, dalla nostra esperienza e dalla nostra ampia rete di partner**

Siamo in una **posizione unica per guidare le trasformazioni digitali**, creare maggiore valore per le nostre persone, i nostri clienti e i nostri partner

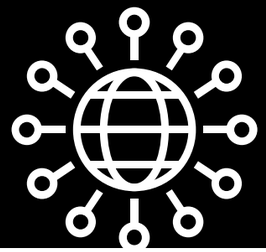
DXC Technology a colpo d’occhio

DXC
LISTED
NYSE

$25B
LEADER GLOBALE
PER I SERVIZI IT

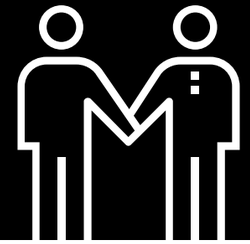
250+
PARTNER

14 STRATEGIC PARTNERS

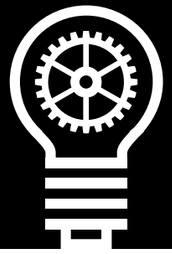


~6,000
CLIENTI

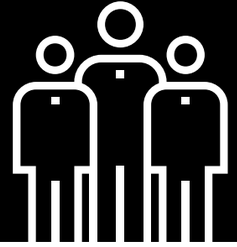
Più di 200 aziende Fortune 500



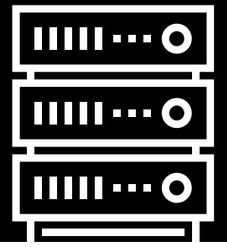
60+
ANNI DI INNOVAZIONE



170,000+
DIPDENDENTI
IN TUTTO IL MONDO



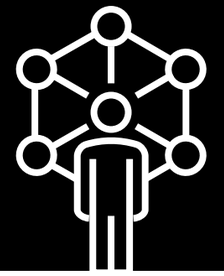
91
DATA CENTER



37
DELIVERY CENTER
STRATEGICI

70+
PAESI

3,600+
PROJECT MANAGER
CERTIFICATI



Agenda

1. I servizi di Cyber Security
2. Perché Agile in un contesto Enterprise
3. Esempio di applicazione di Agile su un progetto di Cyber Security
4. Conclusioni

I servizi di Cyber Security

“La **Cyber Security** è **la protezione delle informazioni** che vengono utilizzate su dispositivi **tecnologici** (e.g. computer, telefoni, IoT, reti). Protezione dall’accesso non autorizzato, dall’abuso, dalla perdita, dalla modifica o la distruzione”

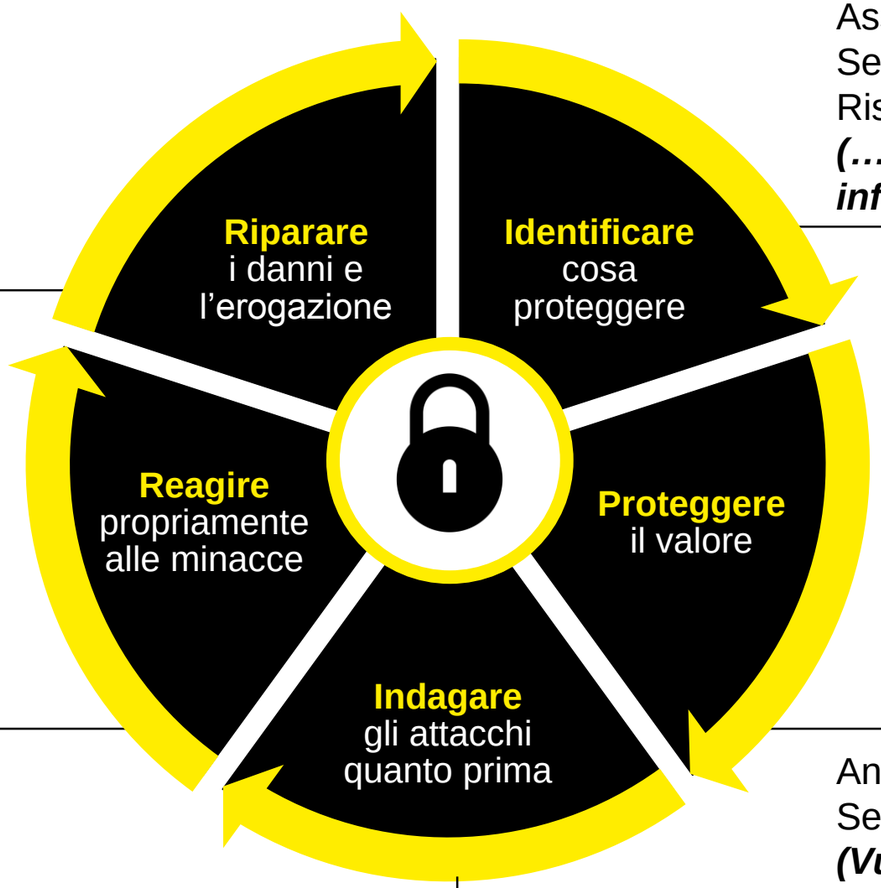
Definizione ispirata a “The Information Technology ACT, 2008”

http://cc.tifrh.res.in/webdata/documents/events/facilities/IT_act_2008.pdf

Il Framework per la Cyber Security

Asset Management
Security Governance
Risk Assessment / Management
(…vulnerability information is received from information sharing forums and sources)

Recovery Planning
Improvements
Communications



Response Planning
Communications
Analysis
Mitigation
(Newly identified vulnerabilities are mitigated or documented as accepted risks)

Identity and Access Management
Awareness and Training
Data Security / Information Protection
(vulnerability management plan is developed and implemented)
Maintenance & Protective Technology

Anomalies and Events
Security Continuous Monitoring
(Vulnerability scans are performed)
Detection

https://www.files.ethz.ch/isn/130080/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20(2)-1.pdf
https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1.pdf

Raccomandazioni dal Framework Nazionale per la Cyber Security

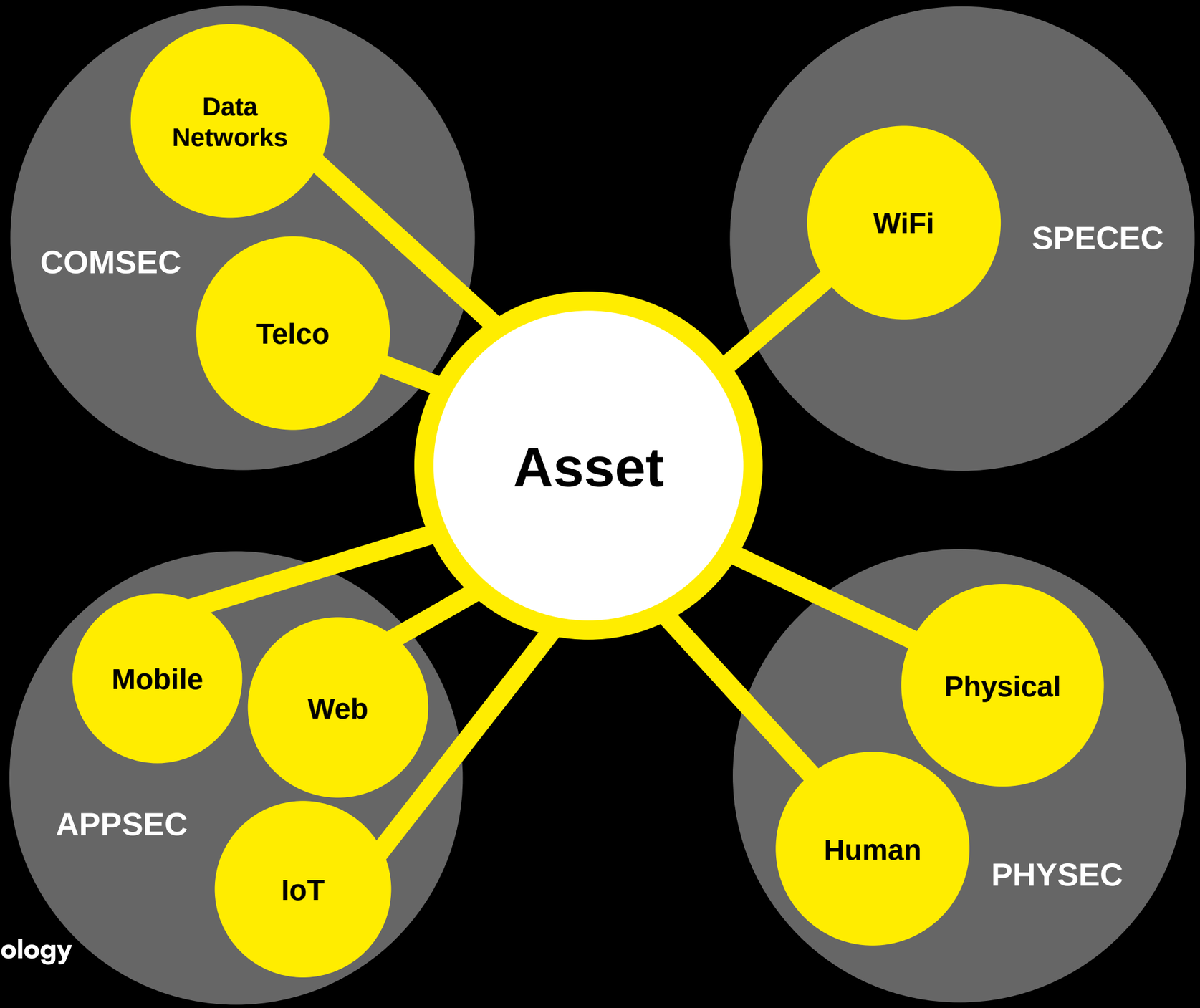
È molto importante, e ampiamente rimarcato dagli esperti che hanno partecipato alla consultazione pubblica, **una estensiva fase di controllo, monitoraggio e valutazione delle vulnerabilità dei propri asset aziendali.**

Nonostante questo documento non preveda un controllo dedicato in modo specifico a questo aspetto, riteniamo che **questo punto debba gradualmente entrare a far parte delle normali routine di controllo** dei sistemi delle imprese**.**

Attività di **threat modeling**, **vulnerability assessment** e **penetration testing permettono di identificare le debolezze dei propri sistemi** […] e per questo **se ne raccomanda l'introduzione** […]

“Un **Penetration Test** è un metodo per la ***valutazione della sicurezza*** tramite la **simulazione di un attacco** dall’interno o dall’esterno”

Definizione di Penetration Test ispirata al CREST



DXC.technology

Inspired by the ISECOM HHS

«Un **Vulnerability Assessment è un metodo per la valutazione della sicurezza** tramite l'utilizzo di strumenti **automatici** che permettono l'identificazione di **vulnerabilità note e comuni** nella configurazione di un sistema»

Definizione di Vulnerability Assessment ispirata al CREST

Attività a confronto

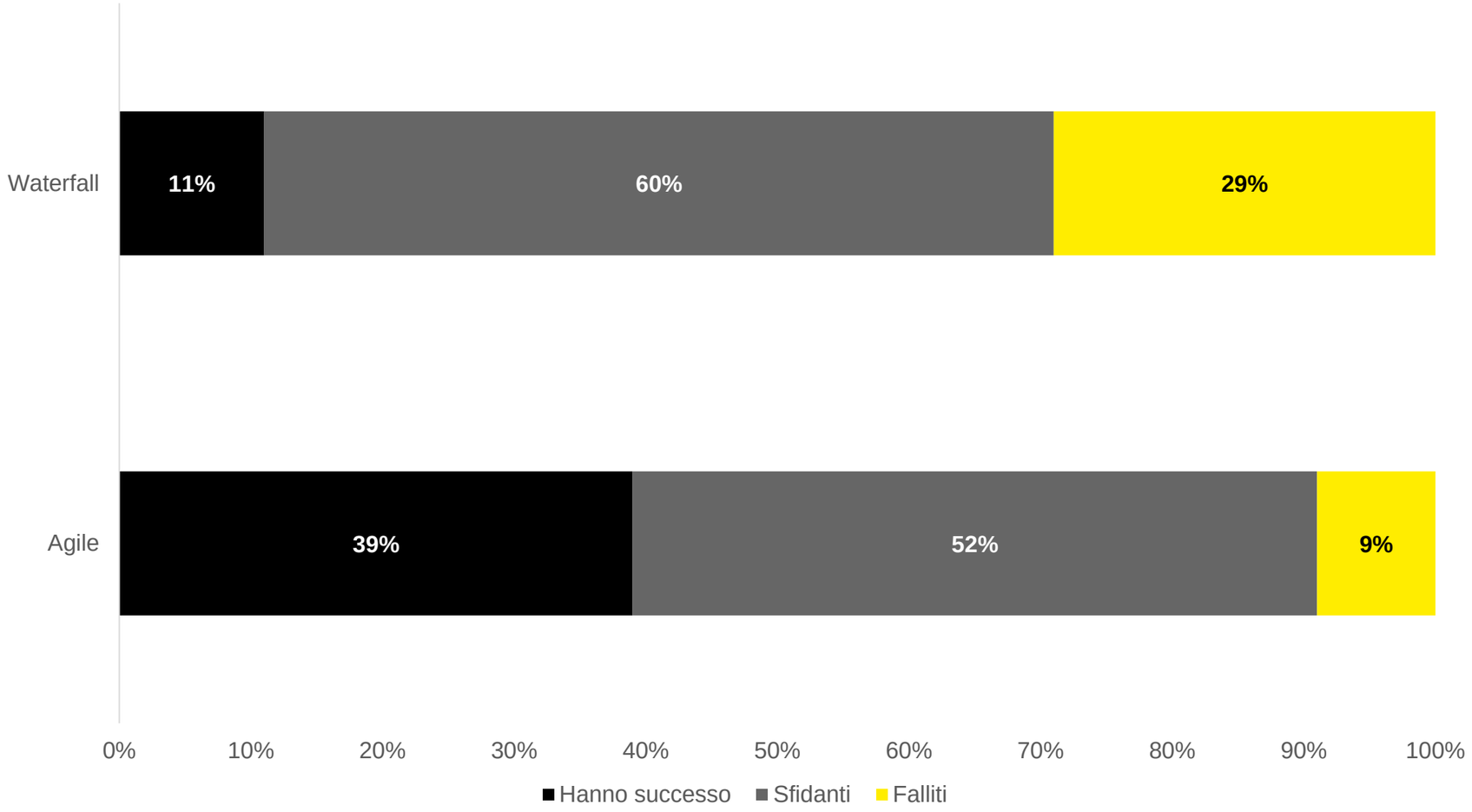
	Vulnerability Assessment	Penetration Test
Scopo	Sono utilizzati per **validare il livello minimo di sicurezza e** come **precursori dei Penetration Test**. Orientato ad una «lista di vulnerabilità note»	Sono utilizzati come **simulazione di un attacco reale**, dimostrando **l'effettiva efficacia del controlli di sicurezza** di un ambiente specifico in un determinato momento. Orientato all'obiettivo.
Modalità di esecuzione	Utilizzo di **strumenti automatici**. Trovano le **vulnerabilità e comuni e già note** (e.g. mis-configurazioni o componenti non aggiornati).	**Approccio manuale** che non si limita alla sola rimozione dei falsi positivi e vanno più in profondità di un VA. Si possono usare strumenti automatici. Normalmente si **sviluppano strumenti ad-hoc**.
Tempistiche	Poco tempo, tipicamente **minuti o ore** per i sistemi; **ore o giorni per le applicazioni**.	**Giorni o settimane**, secondo la **complessità** del bersaglio.

Benefici dei Penetration Test

- **Trovare vulnerabilità** su software, applicazioni, processi, persone per capire:
  - Le vulnerabilità **prima che vengano sfruttate da un attaccante malevolo**.
  - Come mitigarle e quali **controlli implementare**.
  - Se i **controlli implementati** lo siano maniera efficace.
- **Evitare danni alla reputazione**, perdite economiche o d’immagine ecc…

Perché Agile in un contesto Enterprise

Vantaggi dell’essere Agili: più successo



FY2011-2015 CHAOS Report (Progetti Software)

Vantaggi dell’essere Agili: Benefici

Esempio di applicazione di Agile su un progetto di Cyber Security

Come si struttura un Penetration Test: Livello di progetto

Avvio del Progetto

Si inizia con la **Request For Proposal (RFP)**, con requisiti di *alto livello.*
Il primo prodotto è la ***Proposal* del Fornitore** con stima di tempi e costi **.**

I processi utilizzati sono quelli di PRINCE2(R) in una configurazione Agile.

Inizio del Progetto

Si inizia quando la **proposta è accettata.** Insieme al Cliente si fa una **Pianificazione di alto livello e tecnica** almeno della prima fase di consegna. E' necessario avere dei **documenti legali** firmati: CoA e NdA.

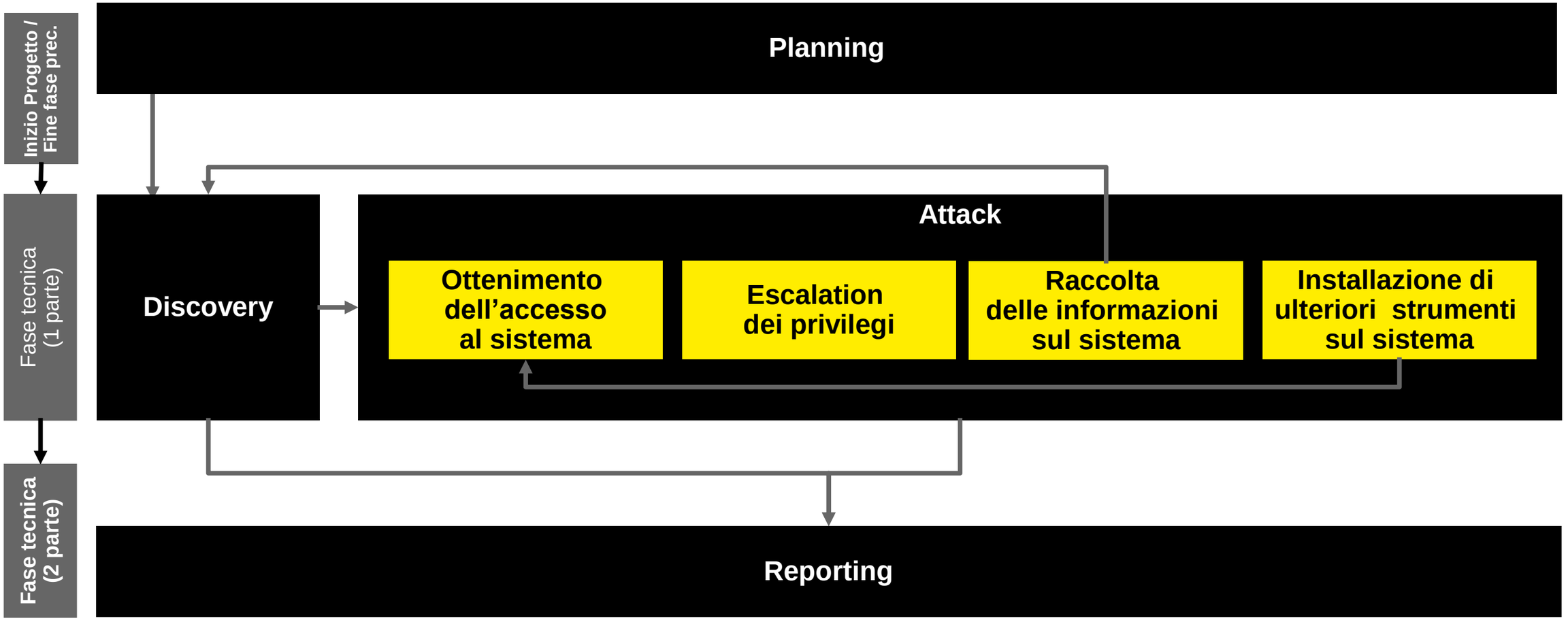
Fasi di consegna

Nelle fasi di consegna si svolgono le **attività tecniche** secondo le metodologie specialistiche necessarie per l'attività specifica.
Ad ogni limite di fase si raccoglie il **feedback** e si **pianifica/rivaluta** il lavoro successivo.

Chiusura del Progetto

Nella chiusura produciamo della documentazione di gestione che ci permette di fatturare, **confermiamo i prodotti consegnati** e procediamo con la distruzione delle informazioni sensibili in nostro possesso.

Come si struttura un Penetration Test: Livello tecnico-specialistico di una Fase di Consegna



Inspired by NIST SP-800-115

Il caso d’esempio: Penetration Test su diversi bersagli

Dettagli sul progetto

Cliente nel settore Banking / Insuriance

Attività di Penetration Testing

Richiesti 8 **deliverable** complessi

Parti coinvolte sul progetto

Fornitore: *team interno* (Sales, Pre-sales, Account & Financial Management, PMO, Delivery) e *team esterno* (altri fornitori)

Cliente: team interno (Sicurezza, IT); team esterno (altri fornitori)

Requisiti iniziali

Budget limitato

Deadline definite dall’alto

RFP senza informazioni rilevanti/non disponibili al Cliente

Mission Impossible

La prima opinione della struttura di Delivery anche in relazione al budget disponibile durante la fase di offerta. La soluzione accettata da tutto il team è stata l’utilizzo del «timeboxing»

Timeboxing e Penetration Testing

La **timebox** è un intervallo di tempo prefissato, una finestra temporale in cui viene creato un incremento di progetto rilasciabile, *potenzialmente* utilizzabile.

- Il **Penetration Test** - per sua natura - **è un processo iterativo**[1] che ha lo scopo di **ottenere**, passo dopo passo, il controllo totale del bersaglio e ben si presta al timeboxing.
- Dal **tempo a disposizione** dipendono il **numero di iterazioni**, la profondità e l'ampiezza della valutazione.
- E' sempre importante considerare che **un attaccante reale** ha in media **146 giorni per portare avanti l'attacco prima che venga scoperto**[2].

[1] NIST SP-800-115
[2] Mandiant M-Trends 2016

Consigli per le stime

Considerare che le persone siano **produttive** per circa **l'80% del loro tempo**.

Le **persone** che lavorano su **diversi progetti contemporaneamente** ci **metteranno più tempo per eseguire le loro attività**, considerando il tempo che viene perso per passare ad attività diverse.

Normalmente le **persone sono ottimiste** nel fare le stime, **quindi sottostimano**.

Stimare usando **l'esperienza propria** e del resto **del team**.

Assicurarsi che la **persona responsabile della creazione del deliverable** sia la **stessa che fa la stima**.

Considerare sempre del **tempo per il problem-solving**, le **riunioni** e gli **imprevisti**.

Stimare la singola attività più che provare a stimare tutto insieme.

Comunicare tutte le **assunzioni**, **esclusioni** e i **vincoli** quando si presenta la stima.

Avvio: stesura della proposta facendo una stima di massima e verificandone la fattibilità

Cosa è successo

Creazione del team: relativo ad una *practice* che ha le caratteristiche necessarie: dinamicità dell'offerta, tipologia delle opportunità, ripetitività delle proposte, maturità del team. Il team è composto solo lato fornitore da persone provenienti da Delivery, PMO, Sales, Presales, Account & Financial Management.
Definizione del business case: del fornitore, rendendolo compatibile con quello del Cliente

La giornata tipica:

- **Stand-up e brainstorming giornaliero** con chi sta lavorando al progetto.
- **Allineamento settimanale** con tutto il team o nei momenti di revisione del lavoro svolto.

Deliverable

Proposal: abbiamo prodotto il documento di Proposal analizzando l'RFP, capendo i benefici che voleva ottenere il Cliente, quindi stima dell'effort (Delivery), economics (Sales), stesura del documento (Presales) e su come gestire la governance (Account & Financial Management) e il progetto (PMO).

Cosa è stato importante

Collaborare: come un unico team inter-funzionale.
Sviluppo iterativo/incrementale: lavorando per brevi iterazioni, rilasciando sempre qualcosa (e.g. effort, cost, price, documento in bozza/rivisto).
Divide et impera: a livello di progetto, abbiamo diviso in elementi di delivery più piccoli.

Inizio: il Cliente accetta la proposta e il nostro scopo è condividere l'approccio e pianificare

Cosa è successo

Cominciano i cambiamenti: una volta accettata la proposta, il team cambia. Ci salutano i colleghi Sales e Presales ed entrano nel team più persone di delivery che dovranno poi eseguire l'attività.

Kick-Off con il cliente: anzitutto incontriamo fisicamente il Cliente. Revisioniamo in maniera critica i deliverable, i fattori di rischio, i tempi e le priorità (considerando in particolare le timebox), i controlli di progetto (e.g. monitoraggio e controllo, accettazione dei deliverable) e le come gestire la parte legale (e.g. mettendo in contatto i reparti legali di ambo le parti).

Definizione della Governance interna: anche in un contesto Agile è importante la governance che sta «sopra» al progetto, abbiamo richiesto degli interventi in momenti specifici e formali con la nostra struttura di Account Management, come da processi interni.

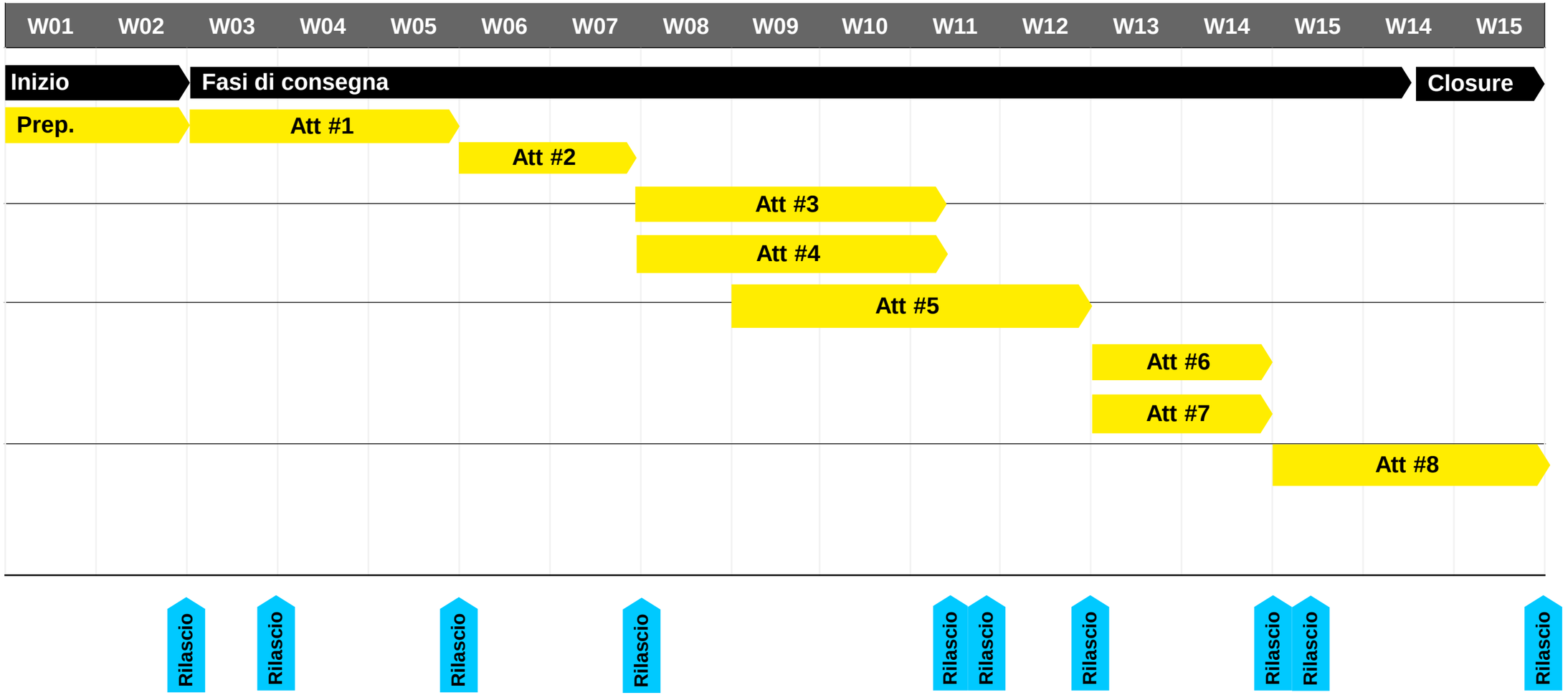
Deliverable

Documento di ambito: Contiene tutte le informazioni relative ai test e la pianificazione. E' un documento «vivo» in quanto Agile.
Non contiene solo il piano di lavoro ma tutti i dettagli (approccio al rischio, alla comunicazione ecc…)

Cosa è stato importante

Collaborazione: coinvolgimento del team *Cliente-Fornitore* per creare «cultura» a garanzia della ripetibilità dell'approccio. Tutte le persone erano già assegnate ad altre attività.
Focalizzazione sul business: coinvolgendo il Cliente per dare la priorità ai vari deliverable.

Il Piano iniziale di alto livello



Fasi di consegna

Cosa è successo

Presupposizioni al piano: le attività preparatorie – in particolare quelle che hanno richiesto il coinvolgimento dei legali – hanno richiesto più tempo del previsto.

Cambio di percorso: delle attività desiderate che richiedevano il coinvolgimento di determinati fornitori: nel *caso migliore* è stato necessario far slittare la i tempi; nel caso peggiore le attività non erano più fattibili.

Importanza dei benefici: col Cliente ci siamo concentrati su come ottenere ugualmente i benefici desiderati cambiando le attività o modificandole e definendo delle priorità in caso di tempi ridotti.

Gestione del tempo: anticipazione delle attività indipendenti; per quelle slittate, anticipazione giornaliera dei risultati, così da avere i benefici quanto prima.

Deliverable

Risultati delle attività di cui:

- **Confermati**: 4 consegnati secondo quanto pianificato o in anticipo.
- **Sostituiti**: 2 realizzazione non praticabile e sostituiti con altri.
- **Modificati**: 2 parzialmente modificati.

Cosa è stato importante

Focalizzarsi sui benefici: e non sui deliverable «in se» o sulle singole attività. Lo scopo di un Penetration Test infatti è di valutare la sicurezza di un determinato bersaglio. E la valutazione si può eseguire secondo diversi tipi di test.

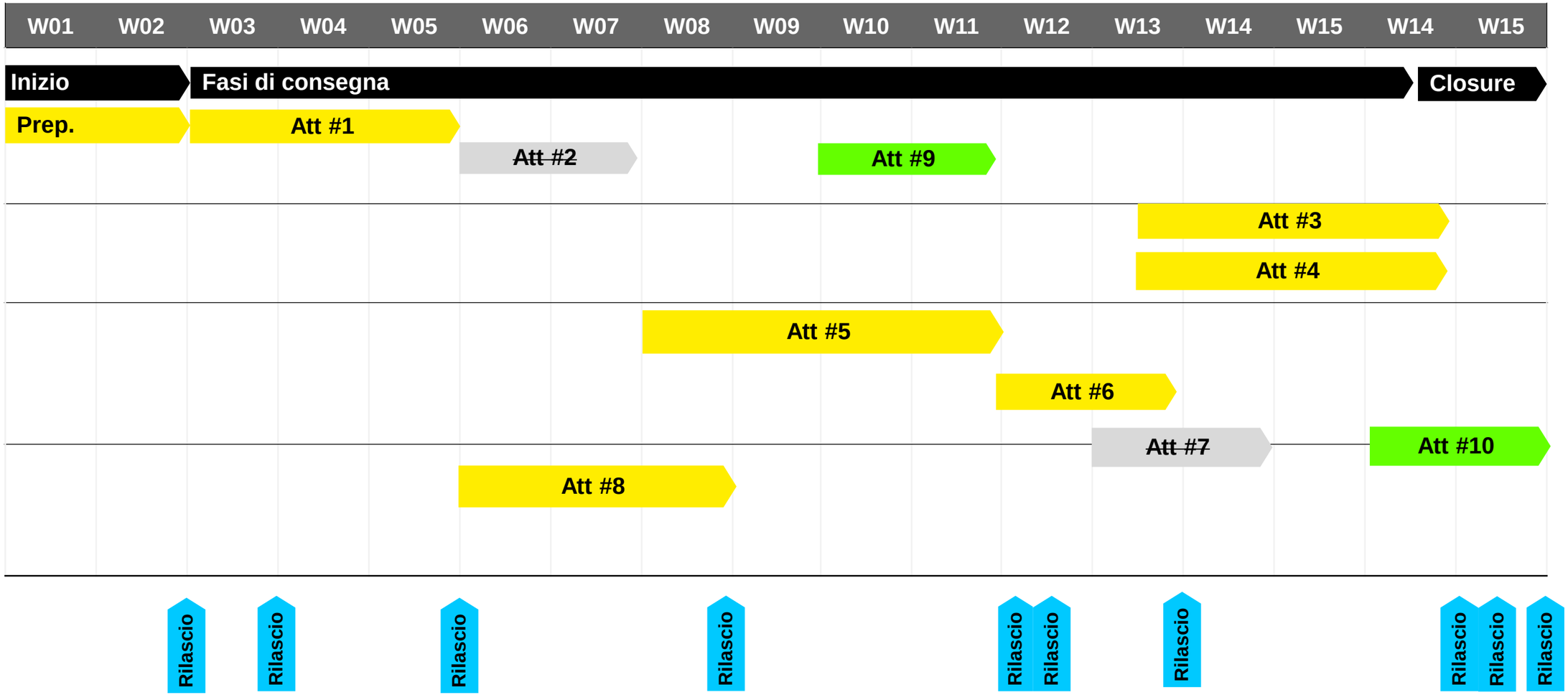
Come è stata strutturata la singola attività

I Tester concordano che l'attività tecnica durerà quindi 8 giornate, il Team Lead concorda col Cliente la clausola della Timebox con l'accordo di allinearsi verso la fine della giornata per anticipare risultati e definire le priorità.

Ogni mattina i tester fanno una chiamata su skype di massimo 15 minuti dove insieme dicono cosa hanno trovato, dubbi e riflessioni, impedimenti che hanno riscontrato e che in caso di necessità sono portati all'attenzione del Project Manager.

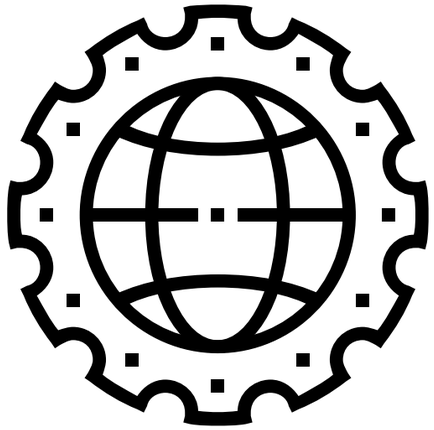
** Le «quick-win» o «low-hanging-fruits» sono quelle vulnerabilità facili da trovare e/o da sfruttare che hanno un impatto alto*

Il Piano finale di alto livello



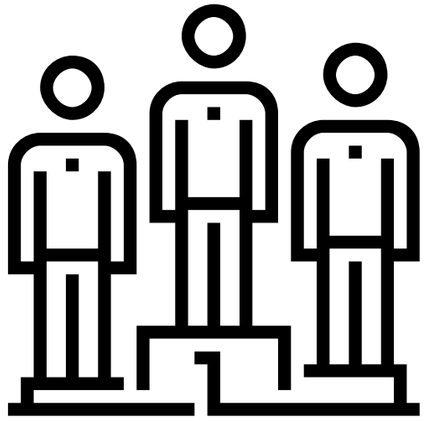
Conclusioni

Lezioni apprese



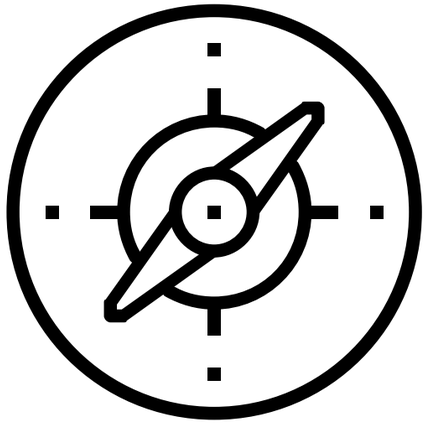
Eccellenza in Agilità

Il Cliente ha risposto al questionario del Net Promoter Score ed è risultato essere un Promotore.



Le persone sono il fattore chiave

Le persone sono il fattore chiave per l’adozione dell’”Agile thinking”. La cultura tipicamente basata su processi e cavilli legali deve cambiare.



Importanza nel Business

Agile è un modello di riferimento per i servizi di Cyber Security, in particolare nei progetti sfidanti.

Grazie.

DXC.technology