



Corso di Laurea Magistrale in Informatica

Security Testing in the Wild: An Empirical Study into the Security Testing Methodologies in Practice

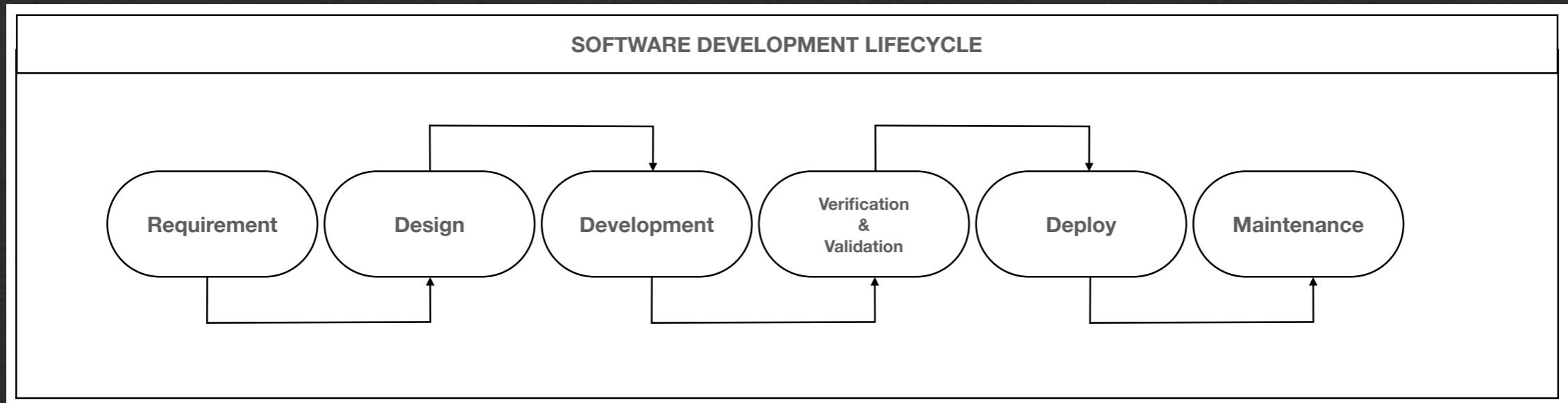
Prof. Fabio Palomba
Dott. Emanuele Iannone
Dott. Stefano Lambiase
Dott.ssa Valeria Pontillo

Dario Di Dario
Mat. 0522500848



Introduzione e Background

SOFTWARE DEVELOPMENT LIFECYCLE

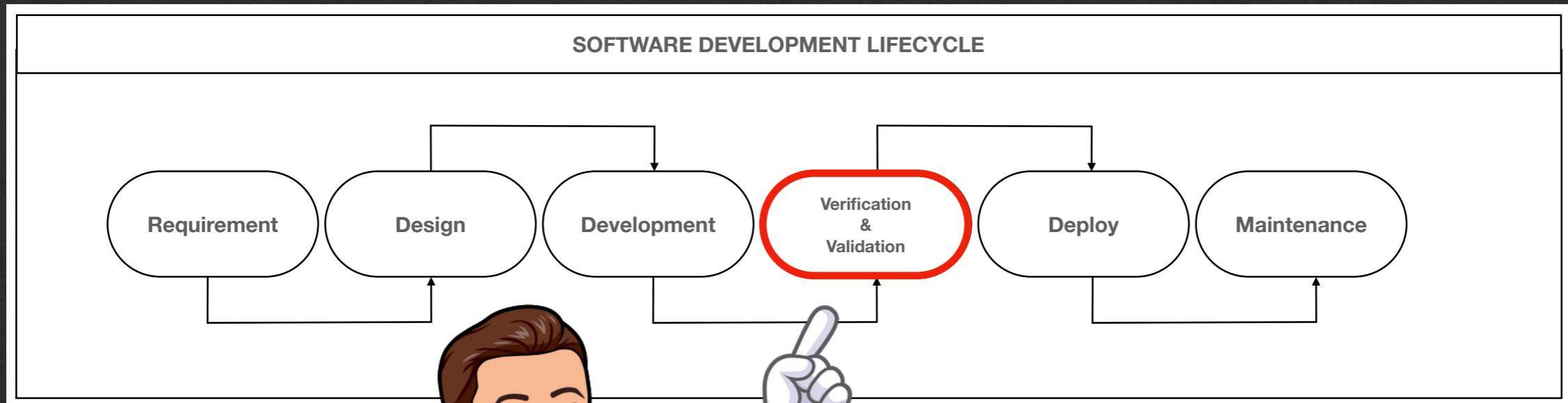


Utilizzato dalle aziende per il design, lo sviluppo e il testing di **software ad alta qualità, soddisfando le aspettative dei clienti.**



Introduzione e Background

SOFTWARE DEVELOPMENT LIFECYCLE



Utilizzato dalle aziende per il design, lo sviluppo e il testing di **software ad alta qualità**, soddisfando le aspettative dei clienti.



Introduzione e Background



Verification: “Am I building the product right?”

Validation: “Am I building the right product?”

- Barry Boehm



Introduzione e Background

***Ma siamo sicuri che il testing
del software ricopra anche
aspetti legati alla sicurezza?***

Verification: “Am I building the product right?”

Validation: “Am I building the right product?”

- Barry Boehm



Introduzione e Background



*Verification is about testing the right product right?
Validation is about getting the right product right?*
- Barry Boehm



Introduzione e Background

VULNERABILITÀ

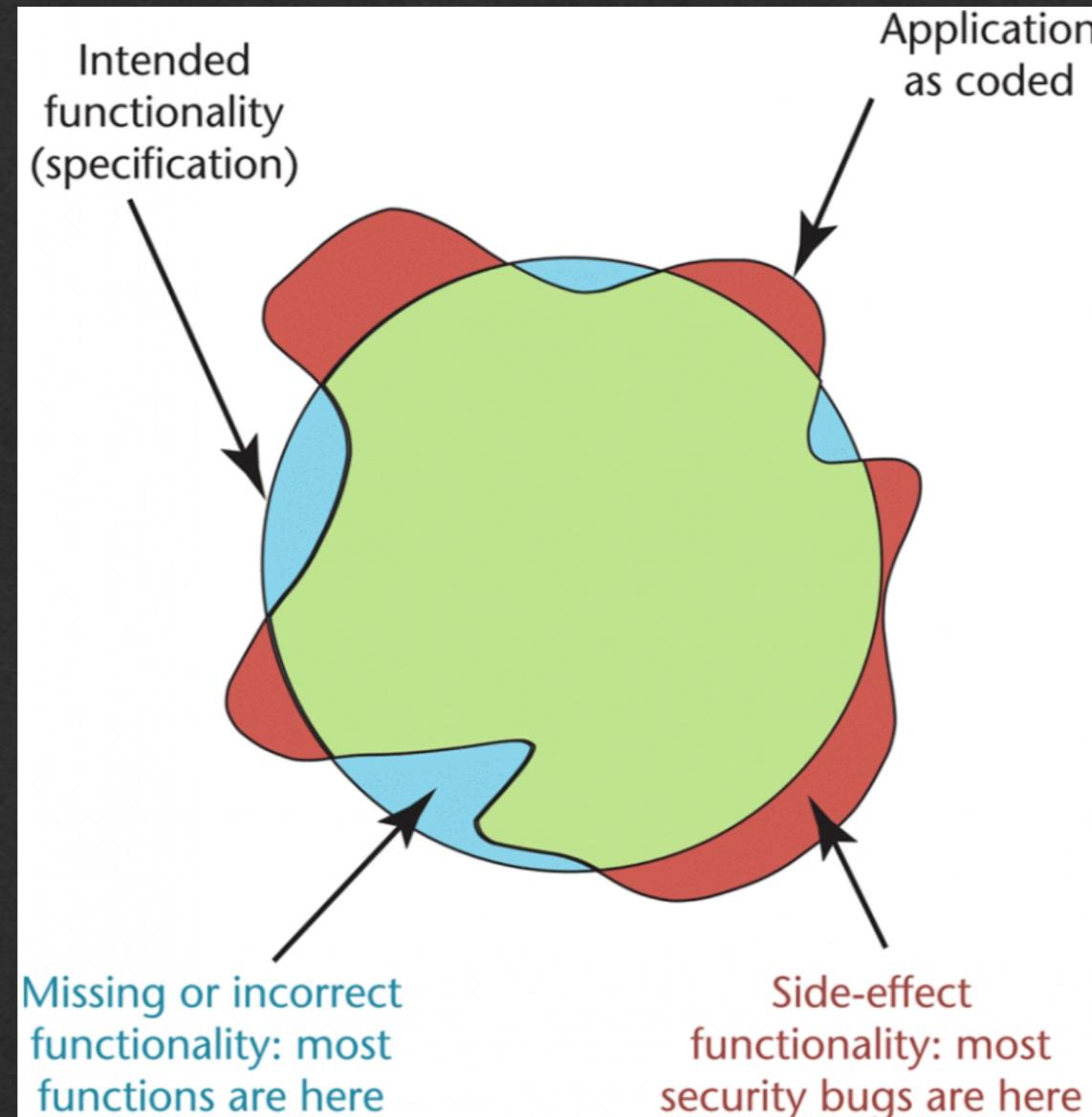
*“A vulnerability is an **instance of fault** in the specification, development, or configuration of the software such that its execution can violate security policy defined within a software organization” **

* Ivan Krsul in “Software Vulnerability Analysis”. ETD Collection for Purdue University (Jan 2011).



Introduzione e Background

EFFETTI COLLATERALI



Introduzione e Background

SECURITY TESTING

Il **Security Testing** è la verifica dei requisiti di sicurezza relativi a proprietà come:

**RISERVATEZZA
DISPONIBILITÀ
INTEGRITÀ
AUTENTICAZIONE
AUTORIZZAZIONE**



Introduzione e Background

SECURE DEVELOPMENT LIFECYCLE

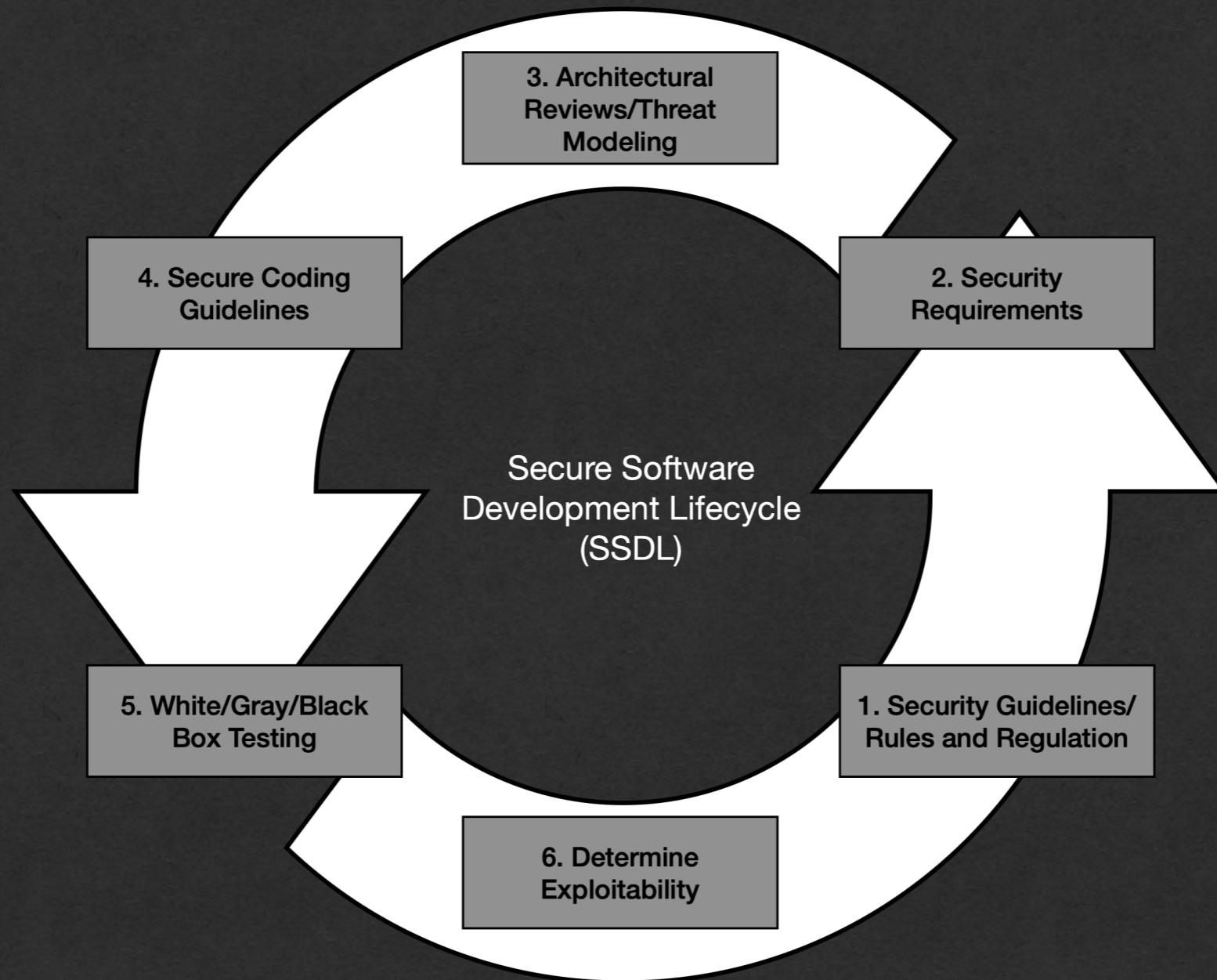


- ✉ d.didario@studenti.unisa.it
- 🌐 <https://github.com/Dariucc07>
- linkedin www.linkedin.com/in/dario-di-dario



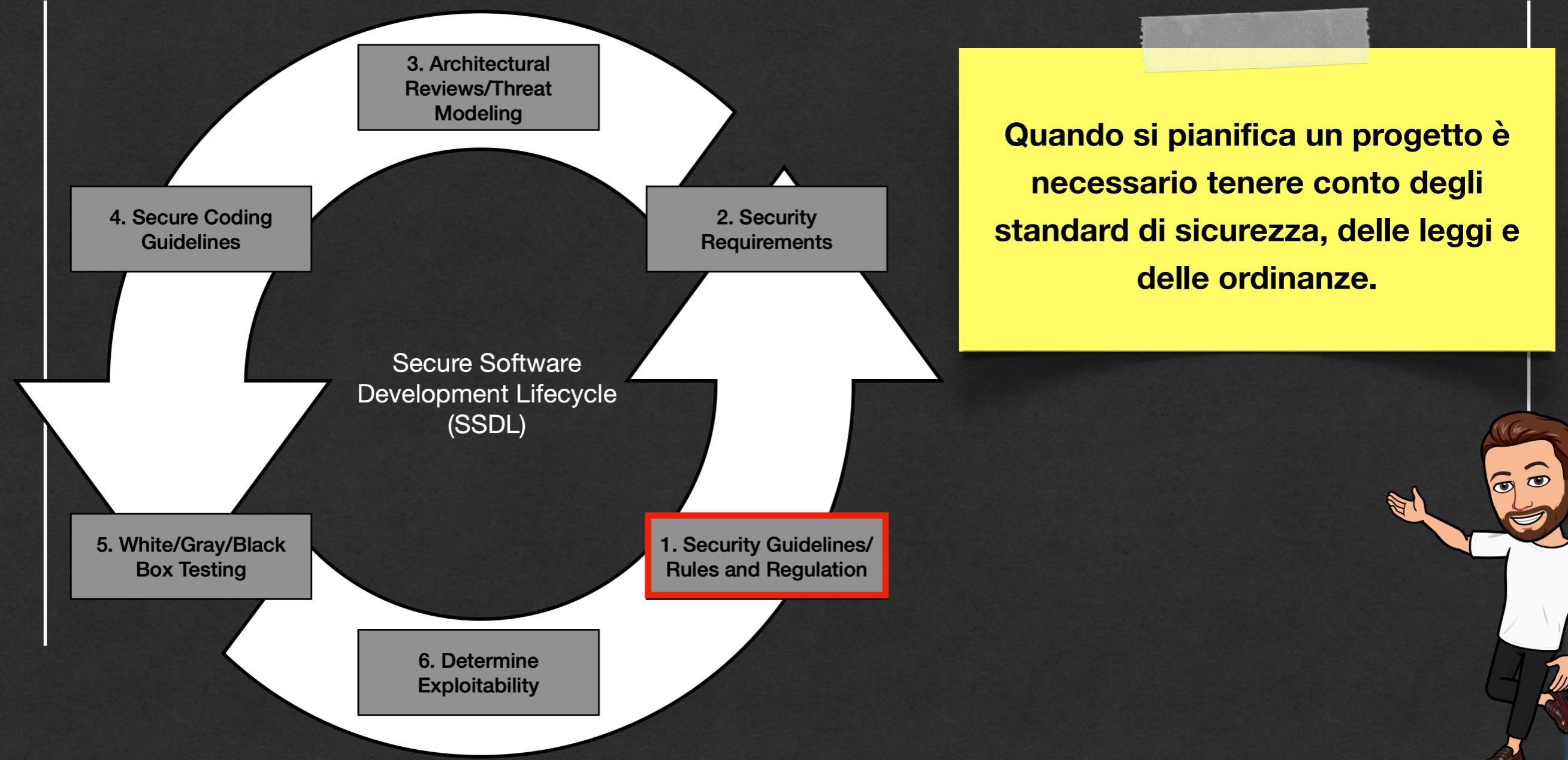
Introduzione e Background

SECURE DEVELOPMENT LIFECYCLE



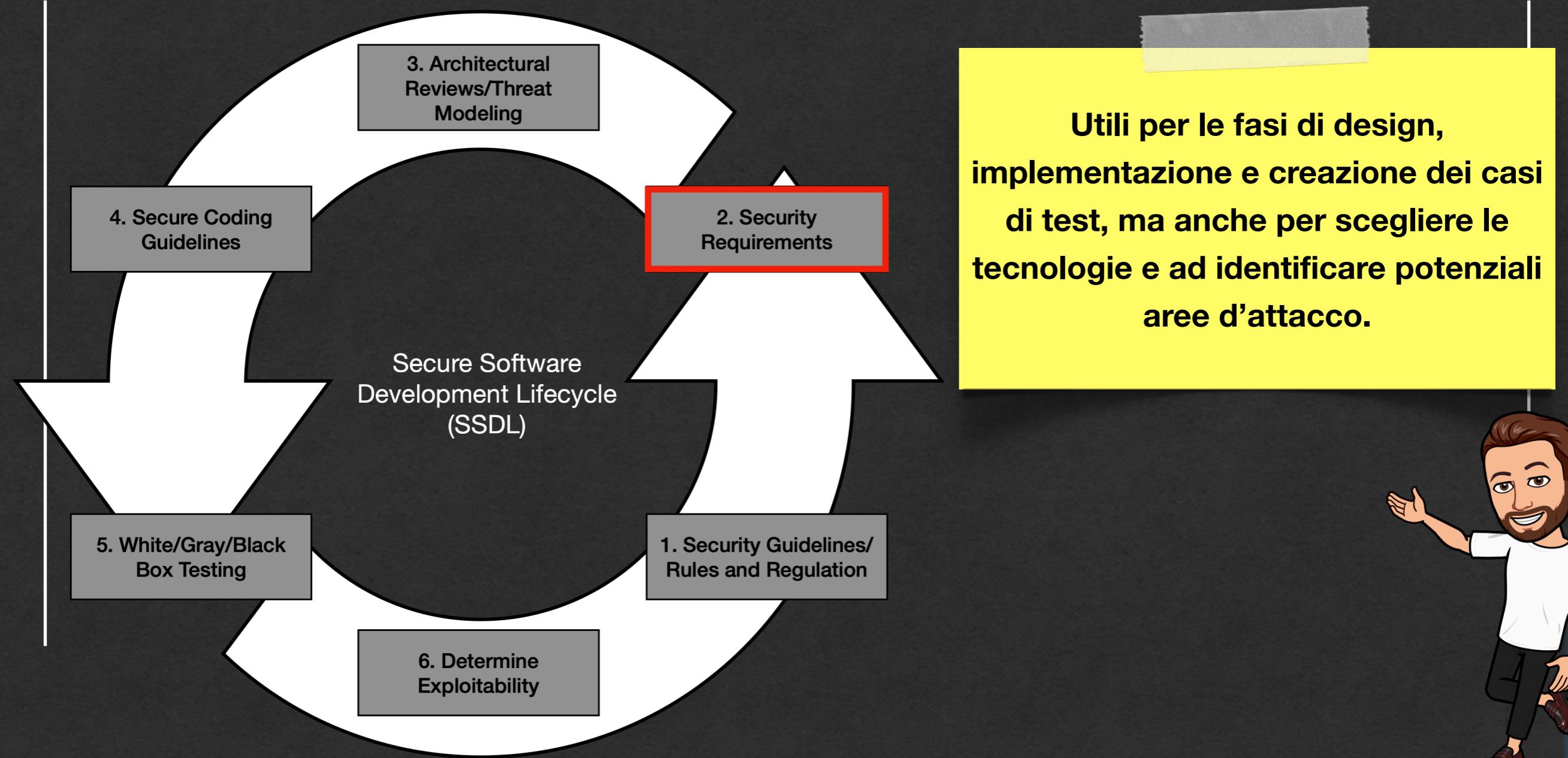
Introduzione e Background

SECURE DEVELOPMENT LIFECYCLE



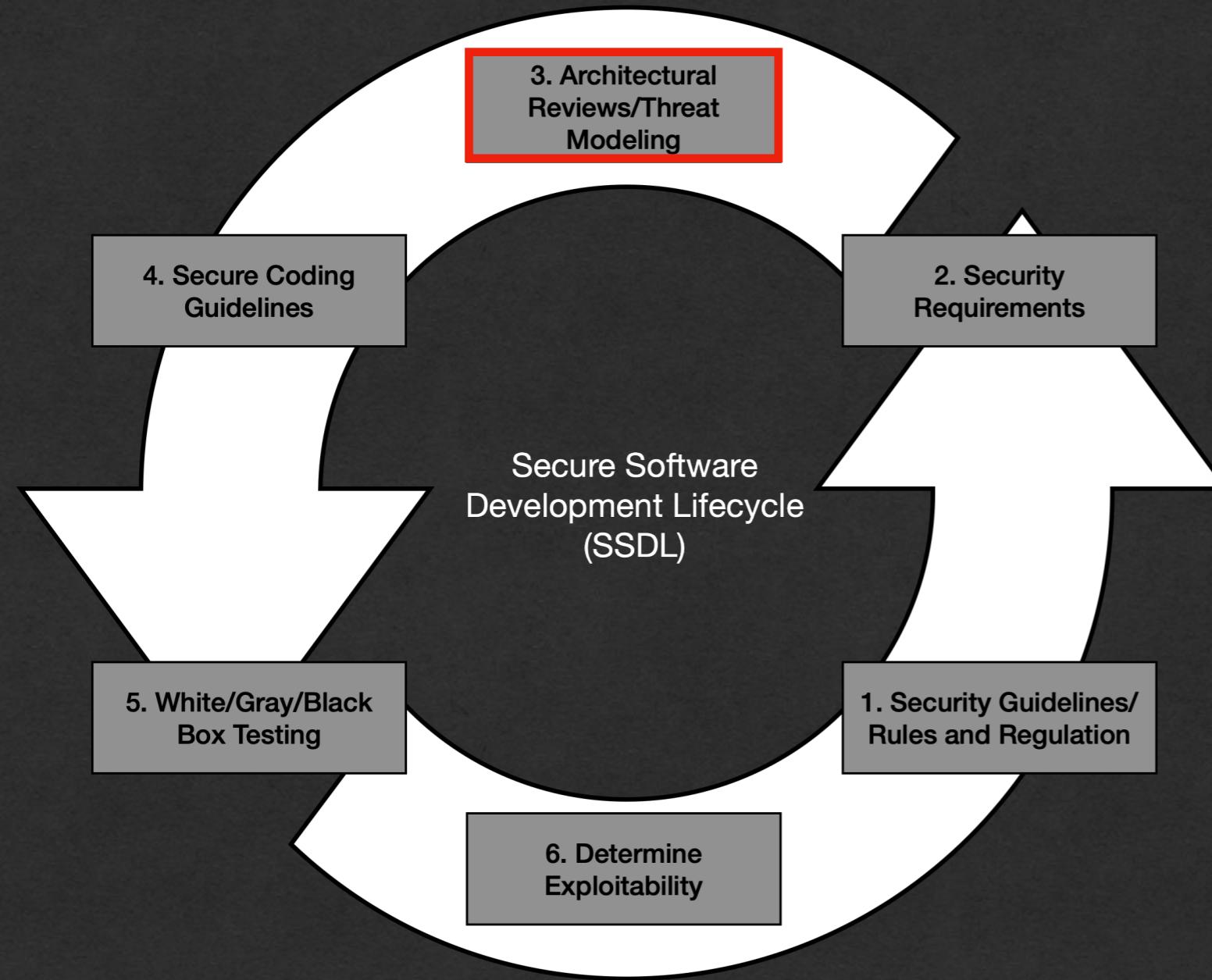
Introduzione e Background

SECURE DEVELOPMENT LIFECYCLE



Introduzione e Background

SECURE DEVELOPMENT LIFECYCLE

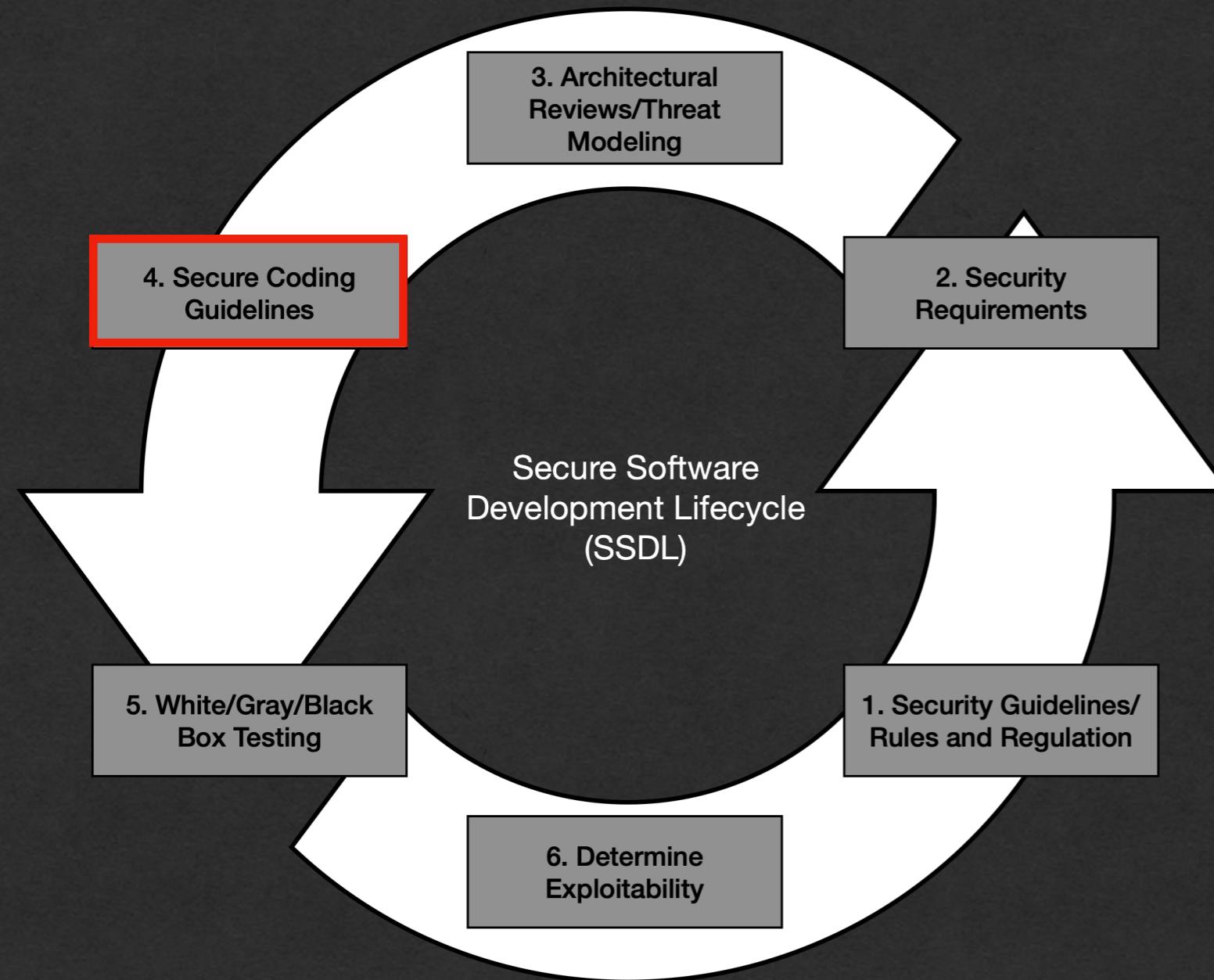


Si identificano potenziali minacce,
come vulnerabilità legate
all'architettura del software,
sviluppando appropriate
contromisure.



Introduzione e Background

SECURE DEVELOPMENT LIFECYCLE

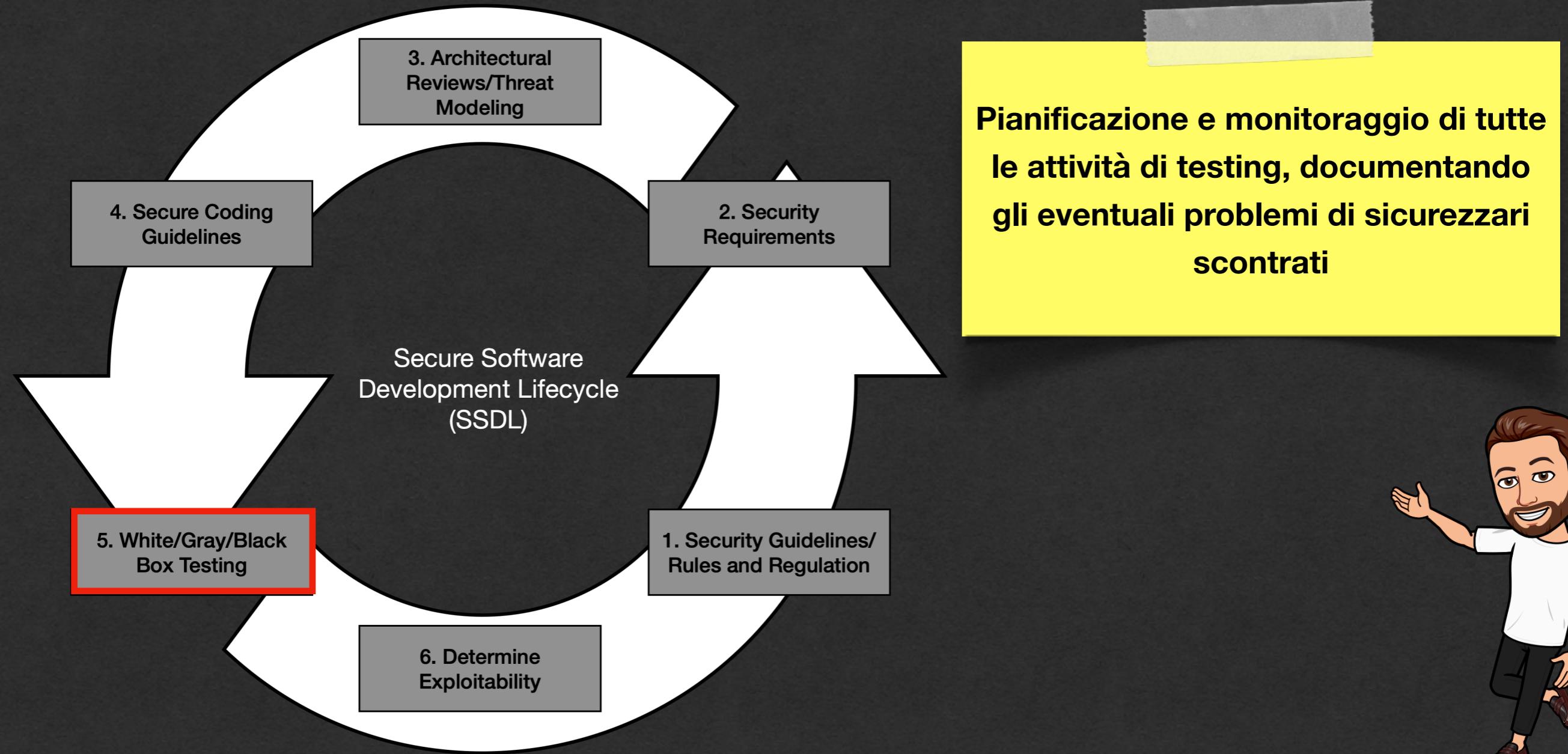


**Static Analysis tools di analisi statica
per evidenziare potenziali
vulnerabilità (e.g., buffer overflow,
ecc.)**



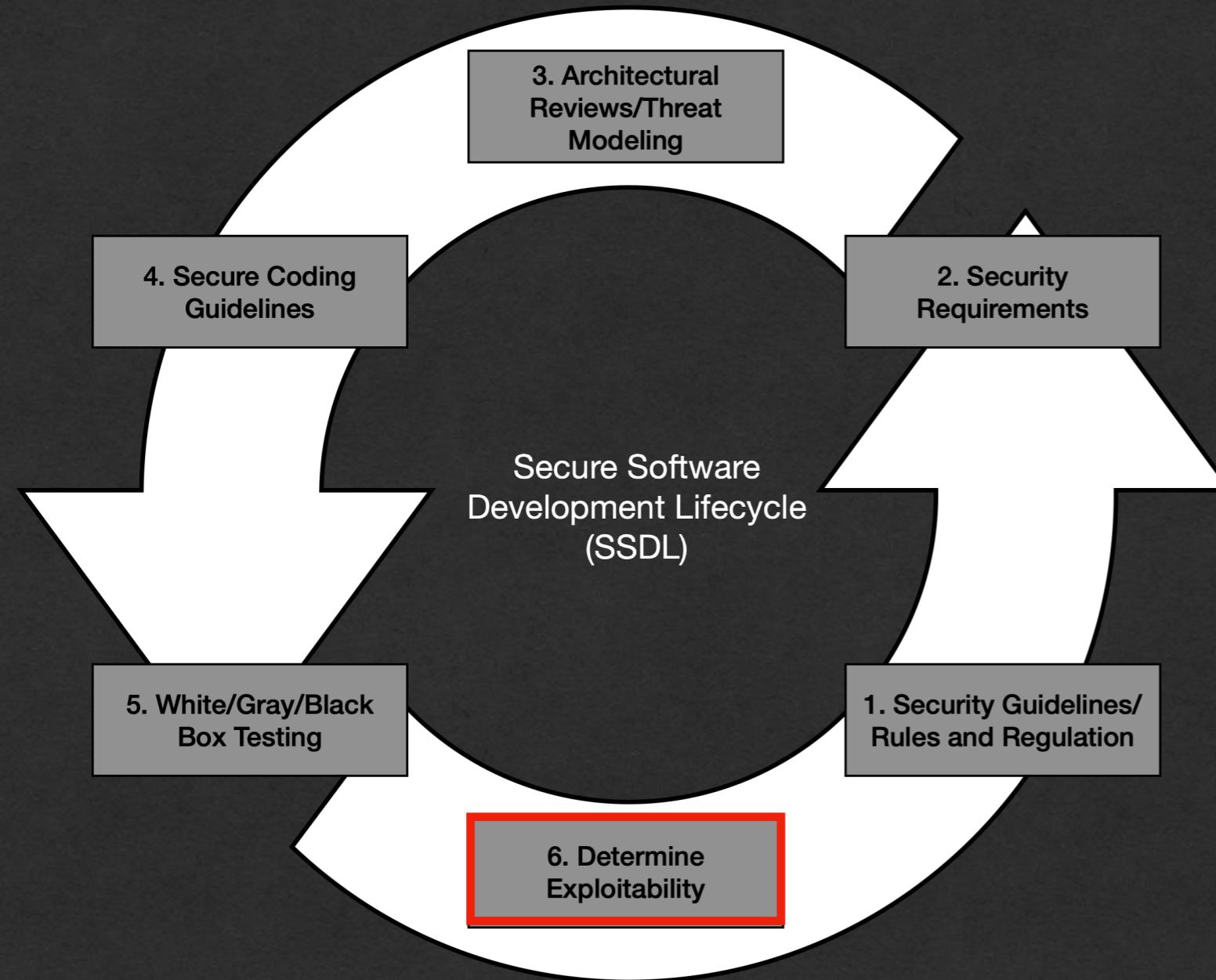
Introduzione e Background

SECURE DEVELOPMENT LIFECYCLE



Introduzione e Background

SECURE DEVELOPMENT LIFECYCLE

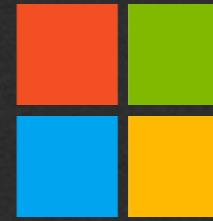


Risolvere i problemi di sicurezza del
passo precedente



Introduzione e Background

SECURE DEVELOPMENT LIFECYCLE FRAMEWORKS



Microsoft

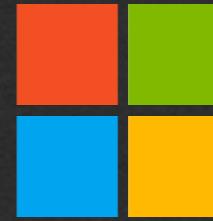


OWASP[®]



Introduzione e Background

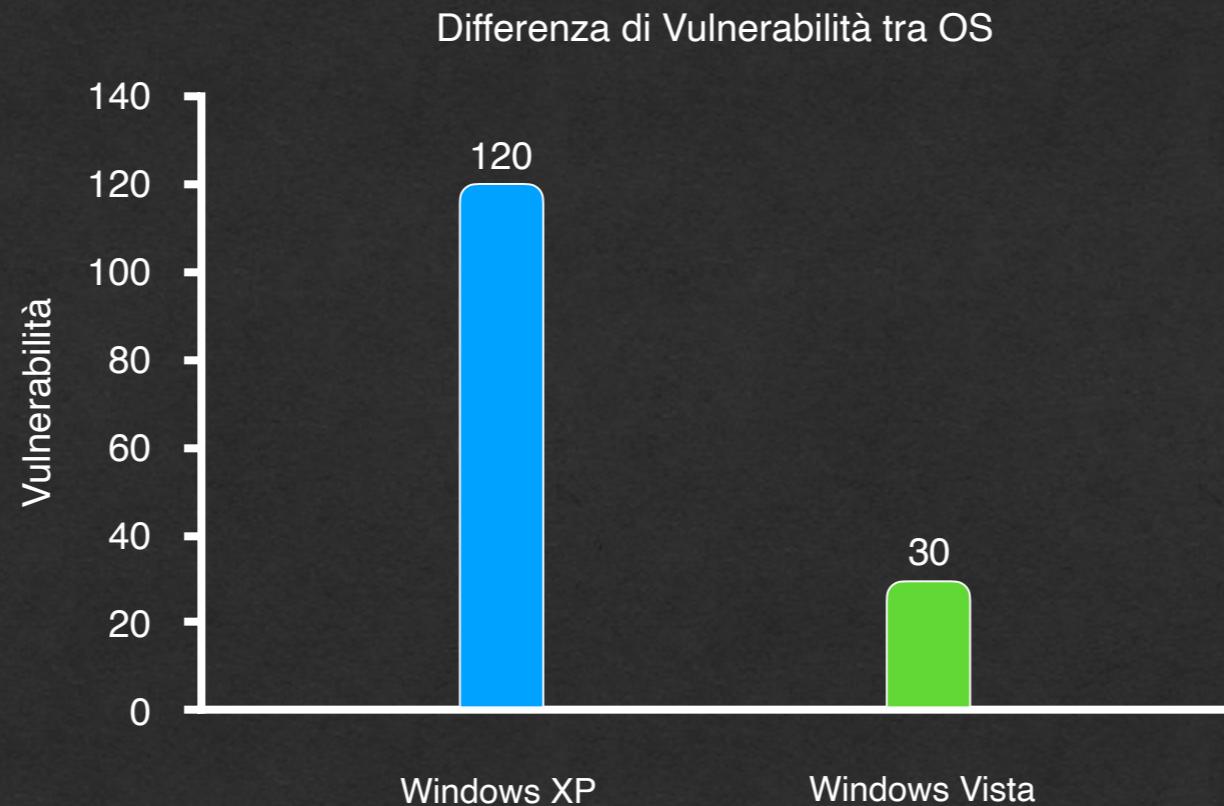
SECURE DEVELOPMENT LIFECYCLE FRAMEWORKS



Microsoft

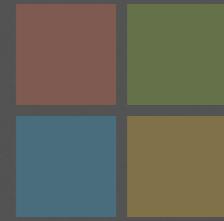


OWASP[®]



Introduzione e Background

SECURE DEVELOPMENT LIFECYCLE FRAMEWORKS

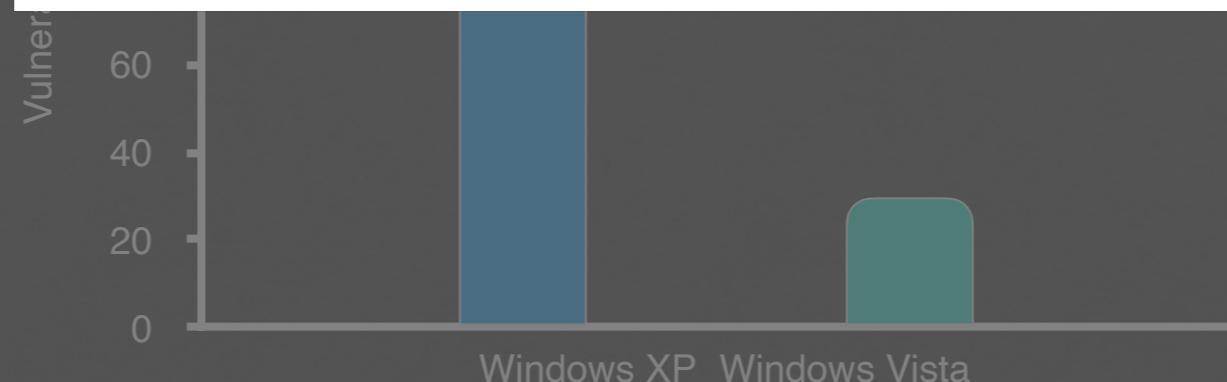


Microsoft



OWASP®

Chi svolge i test di sicurezza?



Introduzione e Background

CHI SVOLGE SECURITY TESTING?

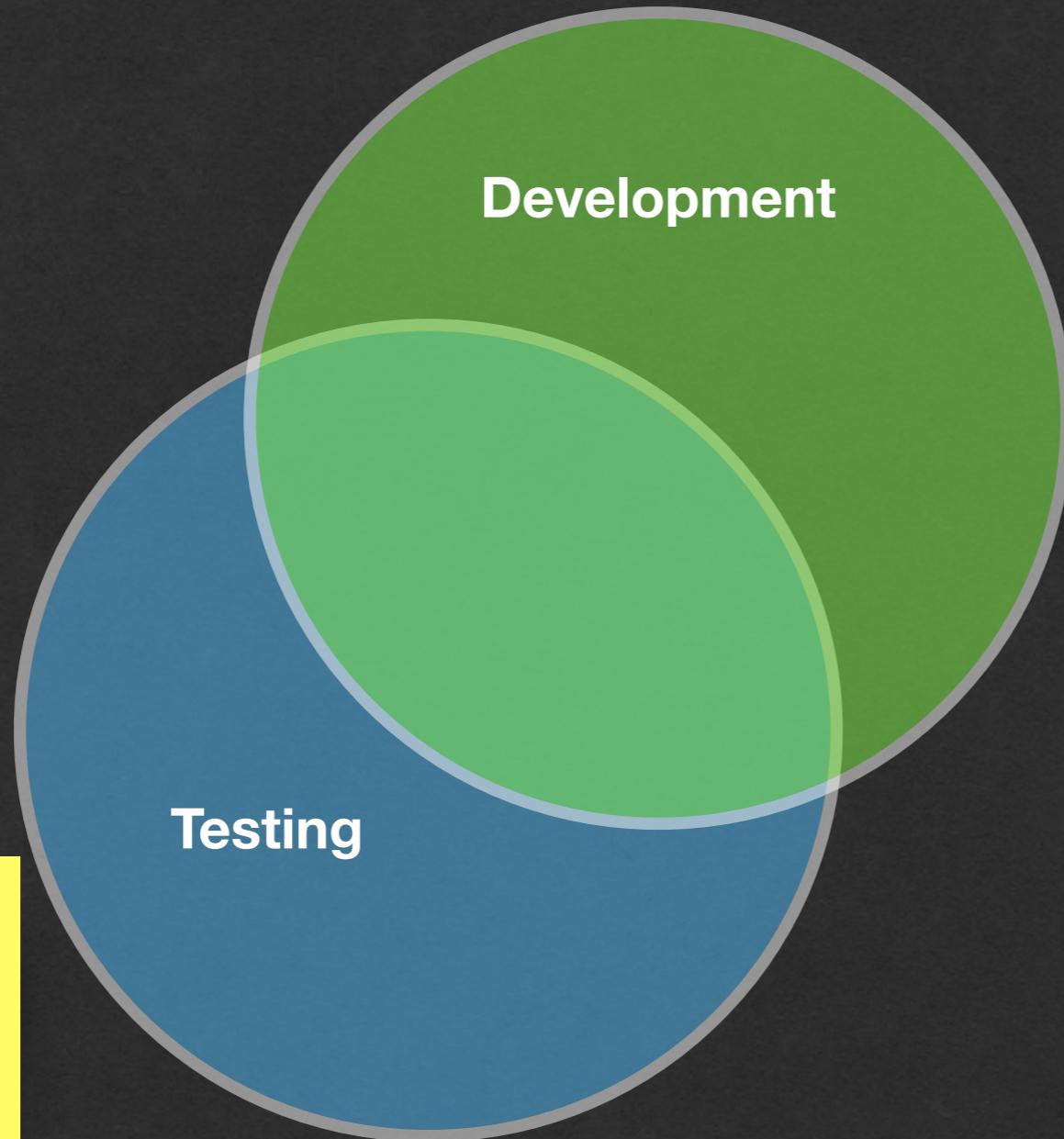
Development

Almeno un linguaggio
ad alto livello



Introduzione e Background

CHI SVOLGE SECURITY TESTING?



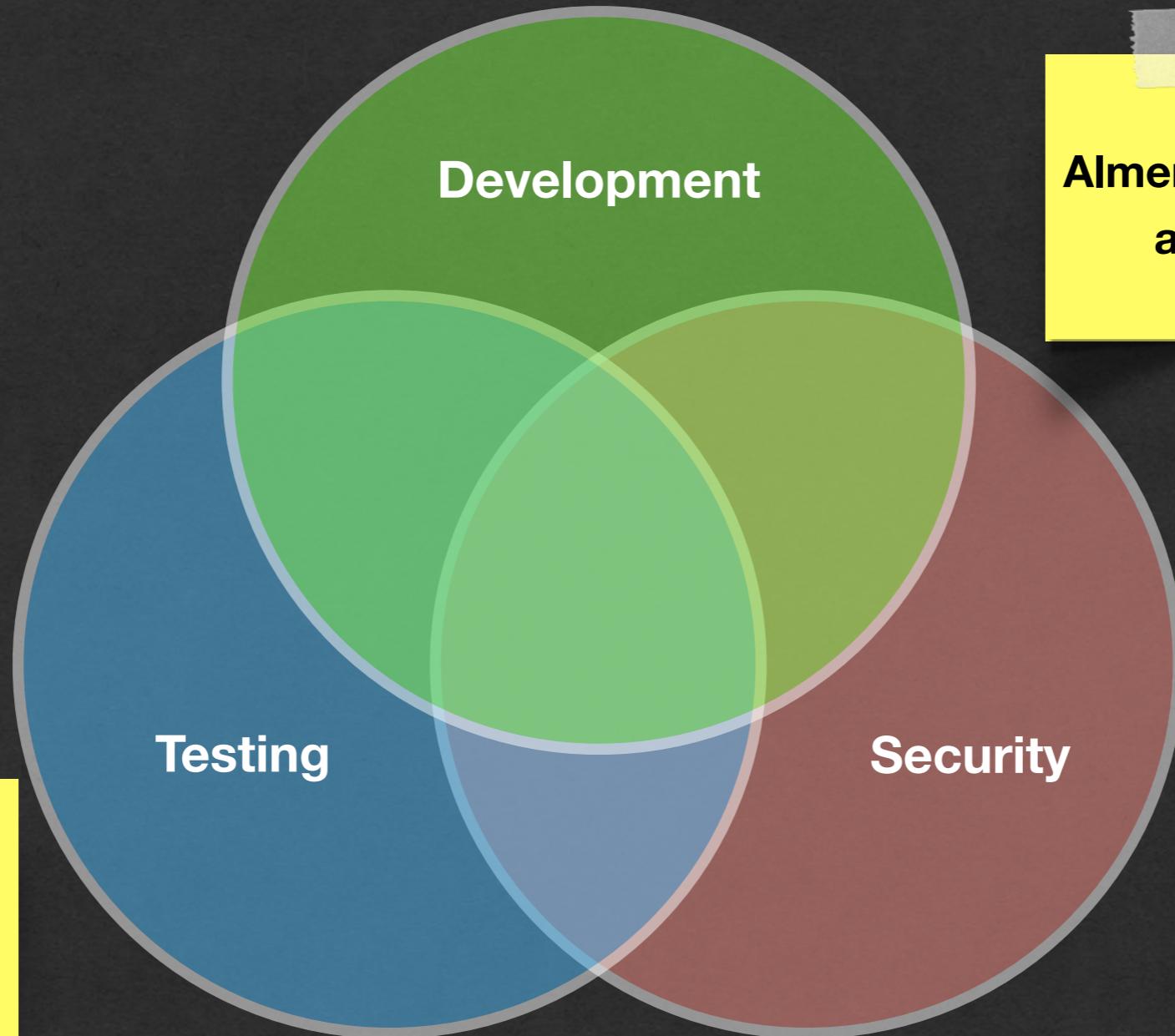
Saper formulare Test
Case Specification

Almeno un linguaggio
ad alto livello



Introduzione e Background

CHI SVOLGE SECURITY TESTING?



Saper formulare Test
Case Specification

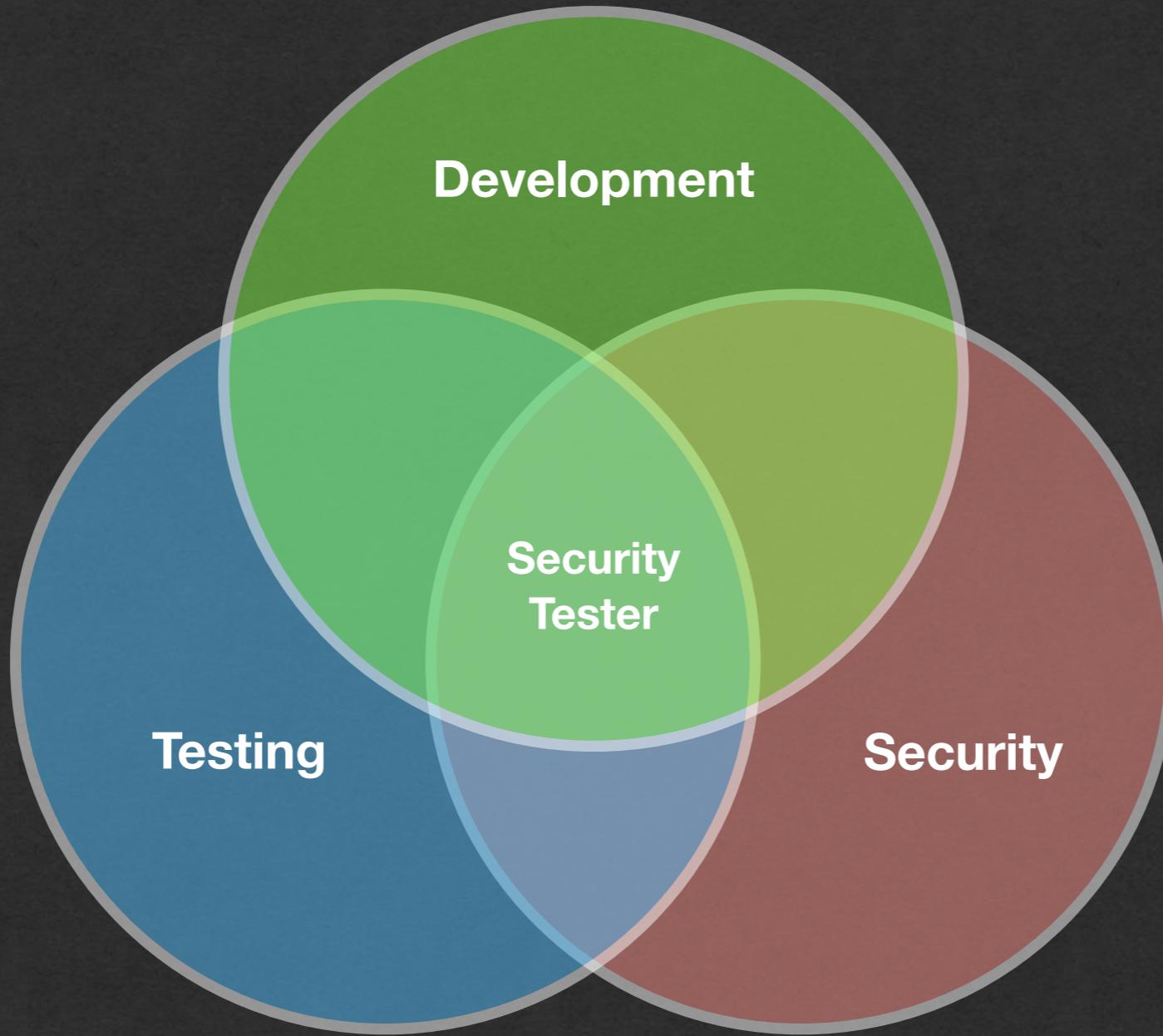
Almeno un linguaggio
ad alto livello

Proprietà di sicurezza
delle soluzioni
implementate



Introduzione e Background

CHI SVOLGE SECURITY TESTING?



- d.didario@studenti.unisa.it
- <https://github.com/Dariucc07>
- www.linkedin.com/in/dario-di-dario



Obiettivi Di Ricerca

Da ciò che si è compreso dall'analisi della letteratura, non è ancora chiaro di come le aziende svolgano attività di **Security Testing**, e se esiste una **figura professionale** che ne svolge e coordina le attività.



Obiettivi Di Ricerca

Da ciò che si è compreso dall'analisi della letteratura, non è ancora chiaro di come le aziende svolgano attività di **Security Testing**, e se esiste una **figura professionale** che ne svolge e coordina le attività.

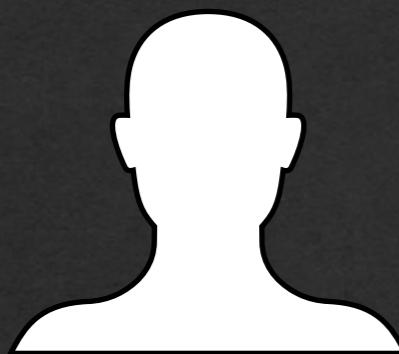
Questo lavoro di tesi vuole fornire il suo contributo tramite una valutazione empirica che si pone i seguenti quesiti di ricerca.



Obiettivi Di Ricerca

Da ciò che si è compreso dall'analisi della letteratura, non è ancora chiaro di come le aziende svolgano attività di **Security Testing**, e se esiste una **figura professionale** che ne svolge e coordina le attività.

Questo lavoro di tesi vuole fornire il suo contributo tramite una valutazione empirica che si pone i seguenti quesiti di ricerca.



Chi svolge
il Security Testing?



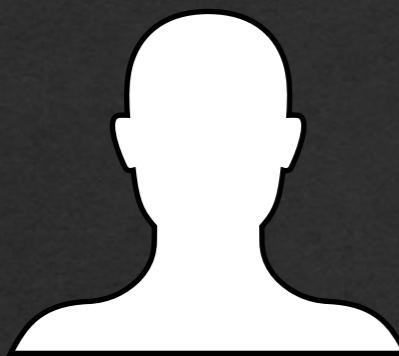
- ✉ d.didario@studenti.unisa.it
- 🌐 <https://github.com/Dariucc07>
- linkedin www.linkedin.com/in/dario-di-dario



Obiettivi Di Ricerca

Da ciò che si è compreso dall'analisi della letteratura, non è ancora chiaro di come le aziende svolgano attività di **Security Testing**, e se esiste una **figura professionale** che ne svolge e coordina le attività.

Questo lavoro di tesi vuole fornire il suo contributo tramite una valutazione empirica che si pone i seguenti quesiti di ricerca.



Chi svolge
il Security Testing?



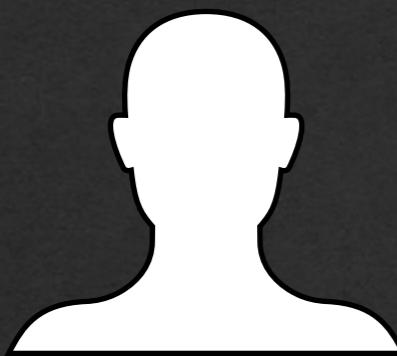
Le aziende sfruttano i
framework di sicurezza?



Obiettivi Di Ricerca

Da ciò che si è compreso dall'analisi della letteratura, non è ancora chiaro di come le aziende svolgano attività di **Security Testing**, e se esiste una **figura professionale** che ne svolge e coordina le attività.

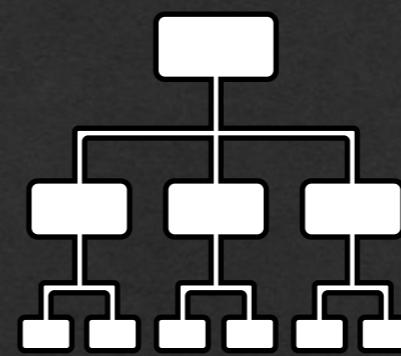
Questo lavoro di tesi vuole fornire il suo contributo tramite una valutazione empirica che si pone i seguenti quesiti di ricerca.



Chi svolge
il Security Testing?



Le aziende sfruttano i
framework di sicurezza?



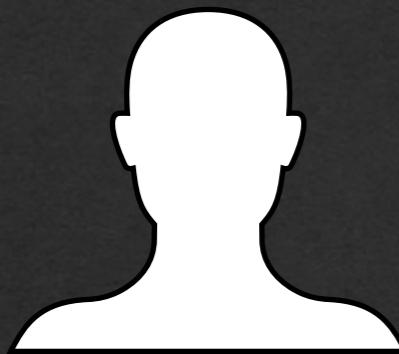
Come sono organizzate
le procedure di security?



Obiettivi Di Ricerca

Da ciò che si è compreso dall'analisi della letteratura, non è ancora chiaro di come le aziende svolgano attività di **Security Testing**, e se esiste una **figura professionale** che ne svolge e coordina le attività.

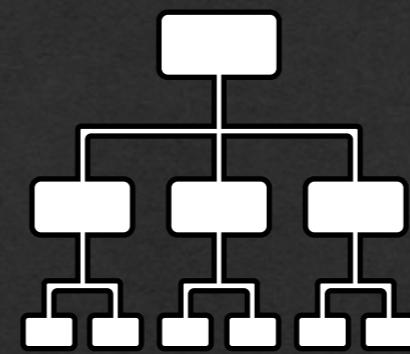
Questo lavoro di tesi vuole fornire il suo contributo tramite una valutazione empirica che si pone i seguenti quesiti di ricerca.



Chi svolge
il Security Testing?



Le aziende sfruttano i
framework di sicurezza?



Come sono organizzate
le procedure di security?



È un lavoro da svolgere
in gruppi di persone?



Metodologia

Per rispondere alle domande di ricerca è stato creato un **Survey** che coinvolgesse Aziende esperte del settore.



Metodologia

Per rispondere alle domande di ricerca è stato creato un **Survey** che coinvolgesse Aziende esperte del settore.



Metodologia

Per rispondere alle domande di ricerca è stato creato un **Survey** che coinvolgesse Aziende esperte del settore.



Metodologia

Per rispondere alle domande di ricerca è stato creato un **Survey** che coinvolgesse Aziende esperte del settore.



Metodologia

Per rispondere alle domande di ricerca è stato creato un **Survey** che coinvolgesse Aziende esperte del settore.



Il professionisti a cui siamo interessanti sono: **Developer, Software Tester, Security Specialist, Senior Manager (CEO, CTO, PM).**



Metodologia

Per rispondere alle domande di ricerca è stato creato un **Survey** che coinvolgesse esperti del settore.



ZUCCHETTI



ERIA INFORMATICA

Il professionista
Software (Analista,
CTO, PM).

Perchè un Survey?



Metodologia

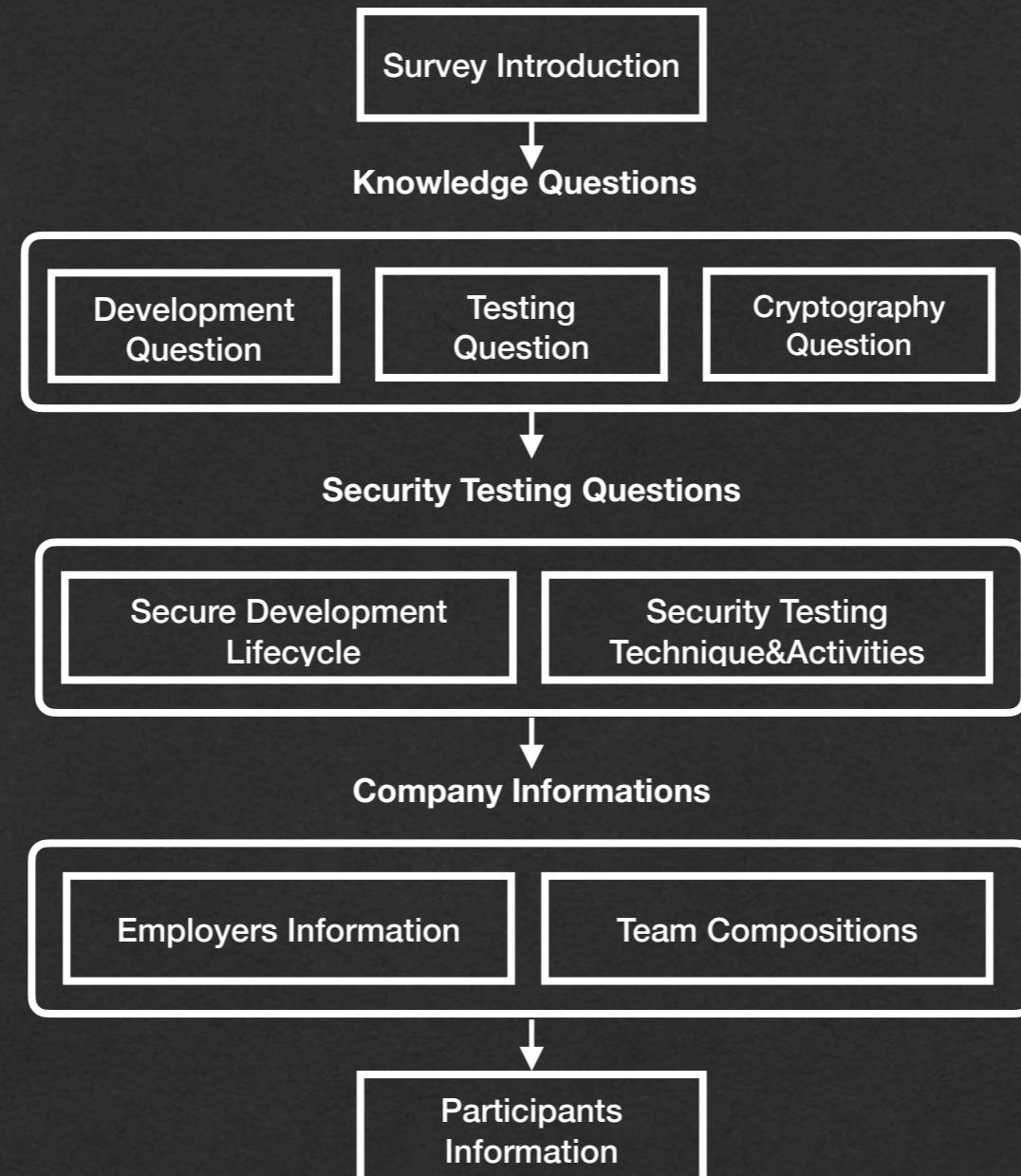
Per rispondere alle domande di ricerca è stato creato un **Survey** che coinvolgesse esperti del settore.

Perchè?

- (1) Coinvolge in modo mirato uno specifico gruppo di candidati.
- (2) Integra differenti culture e background.
- (3) Ottiene rapidamente dati omogenei e facili da analizzare.

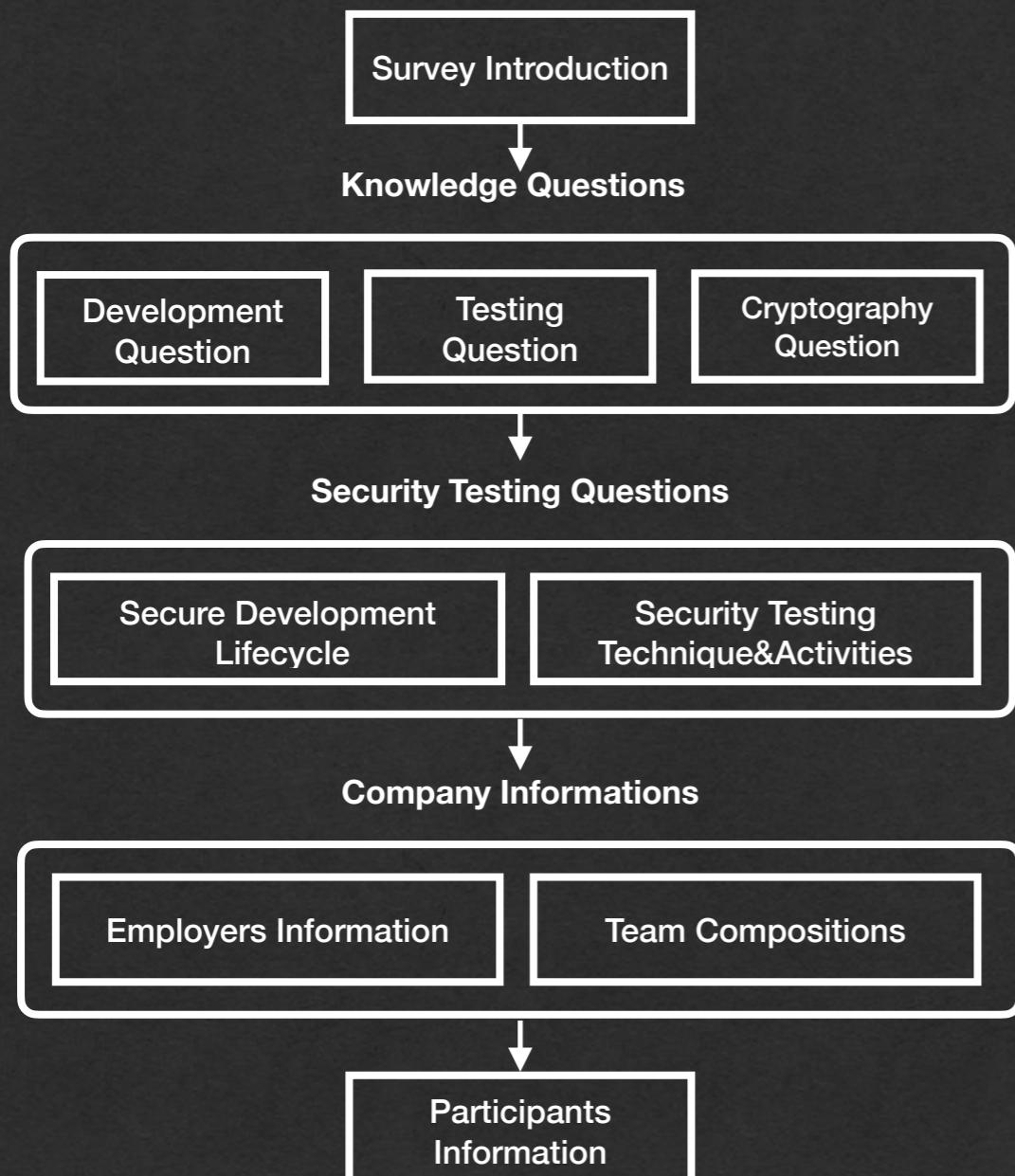


Metodologia



Metodologia

DETTAGLI STUDIO EMPIRICO



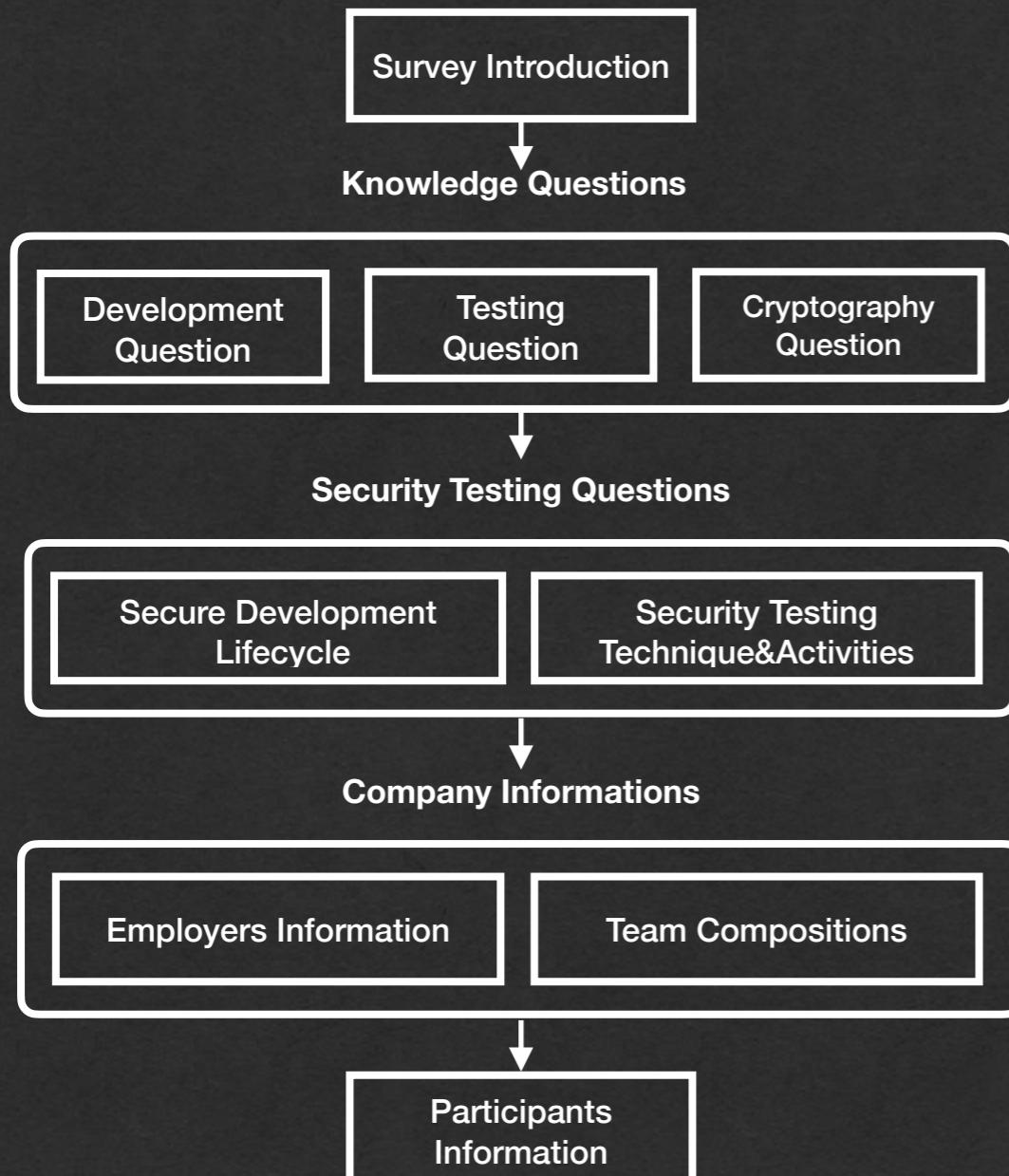
Condotto un **Test Pilota** con studenti lavoratori per verificare la chiarezza delle domande.

Inviato alle aziende tramite **Google Form**.



Metodologia

DETTAGLI STUDIO EMPIRICO



Condotto un **Test Pilota** con studenti lavoratori per verificare la chiarezza delle domande.

Inviato alle aziende tramite **Google Form**.

Data Quality Pre-Screening per validare le risposte.

26 risposte totali di cui 19 analizzate.



Metodologia

INTERVISTA INDIVIDUALE



ZUCCHETTI



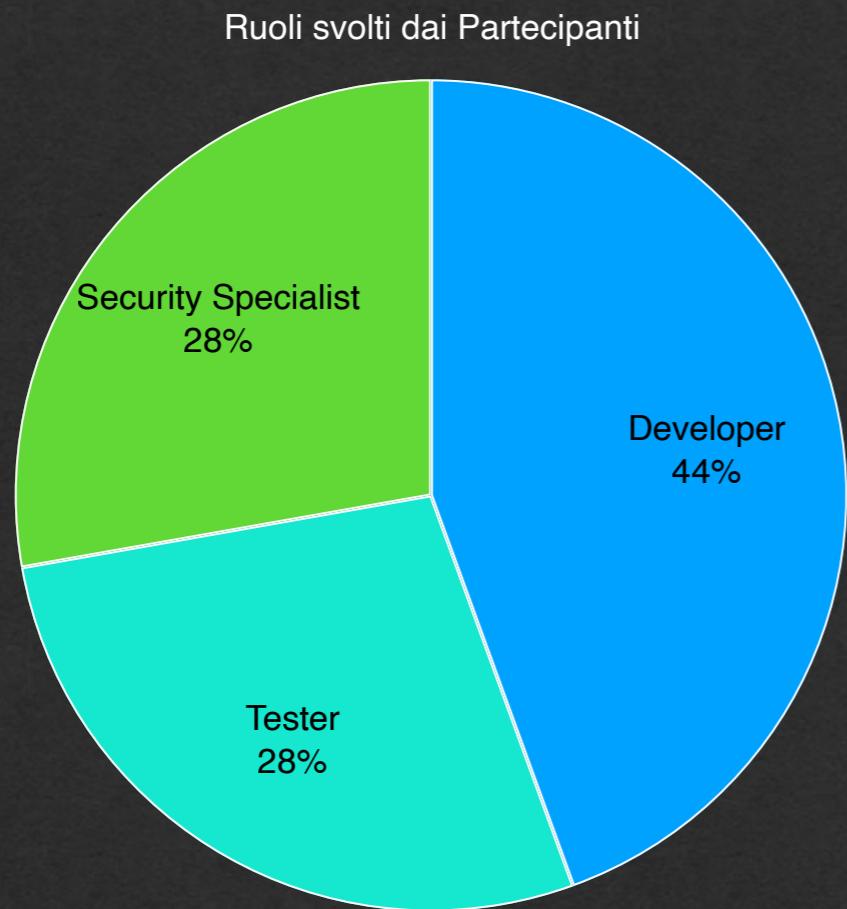
Gregorio Piccoli, *CTO*
Zucchetti

Arricchendo ulteriormente le informazioni ottenute dalle singole risposte.



Risultati Di Ricerca

DATI AZIENDALI E PERSONALI

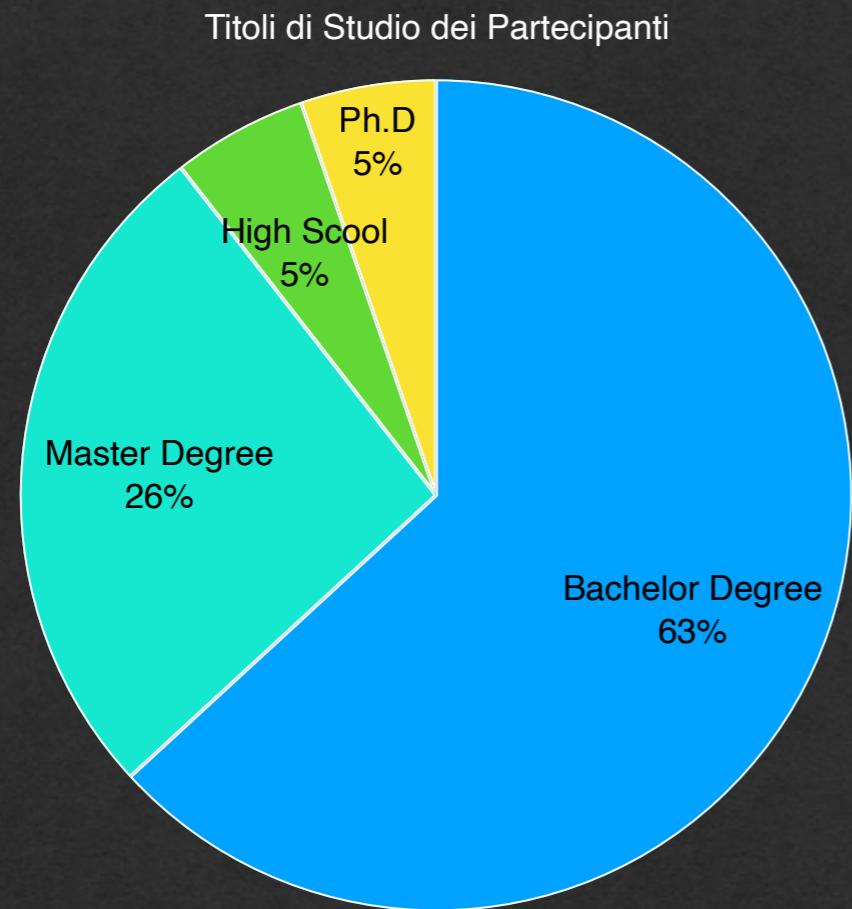


Il 44% dei partecipanti svolge il ruolo di **Developer**. Il 28% è un **Security Specialist**. Il 28% rimanente svolte **Software Testing**



Risultati Di Ricerca

DATI AZIENDALI E PERSONALI

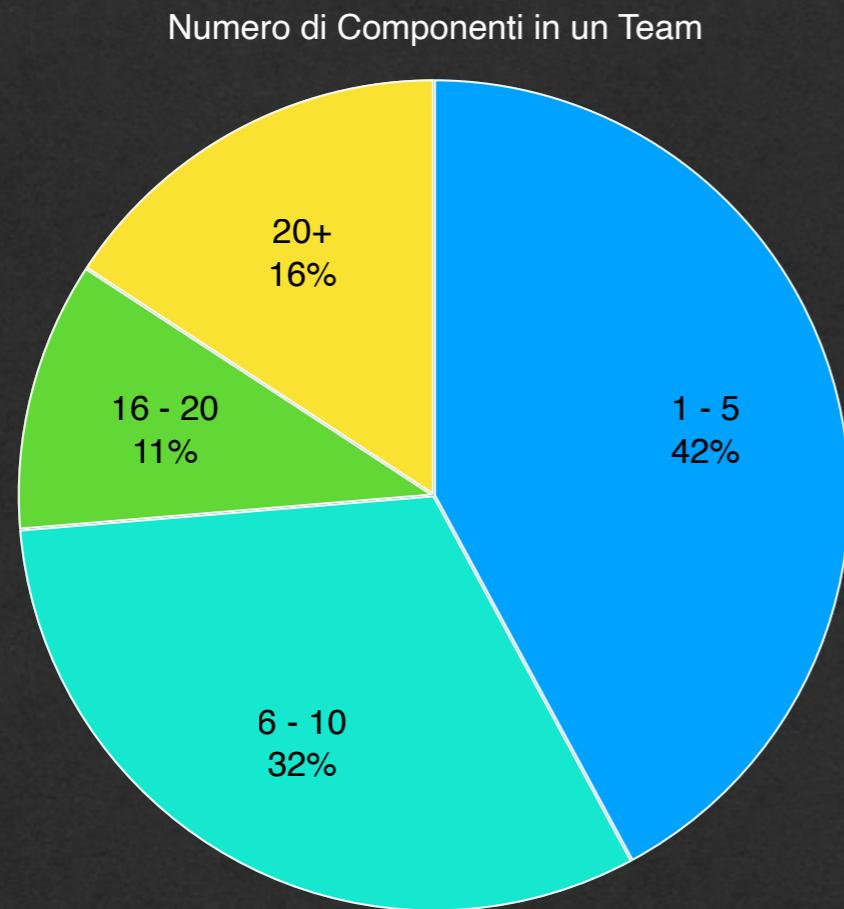


Il 63% dei partecipanti ha conseguito la **Laurea Triennale in Informatica**. Il 26% ha conseguito la **Laurea Magistrale in Informatica**. Il 5% ha conseguito il **Diploma di scuola superiore**. L'ultimo 5% ha conseguito il **Dottorato di Ricerca**.



Risultati Di Ricerca

DATI AZIENDALI E PERSONALI

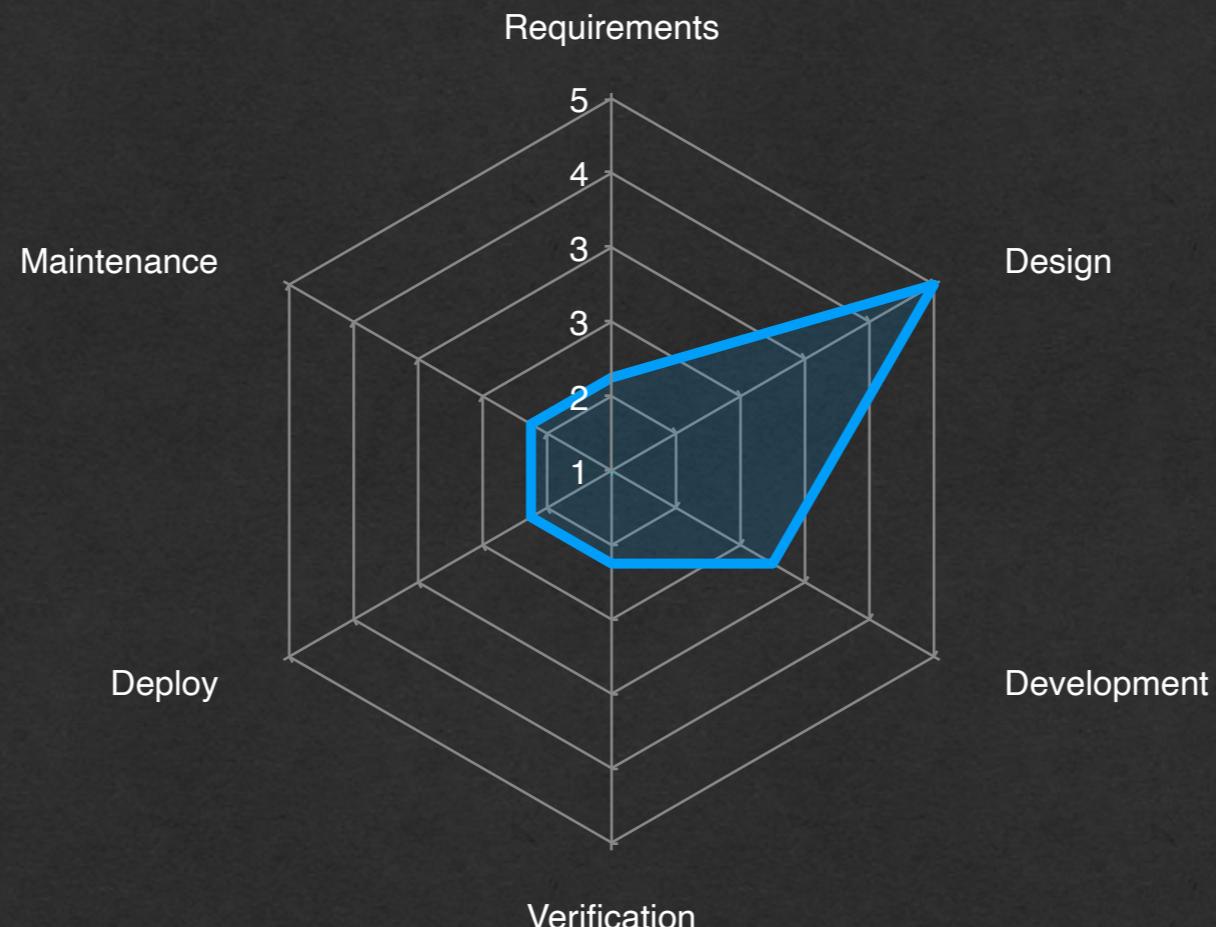


Il 42% dei partecipanti lavora in un team composta da **1 a 5 persone**. Il 32% in team composti da **6 a 10 persone**. I rimanenti da **16 a 20 e più persone**.



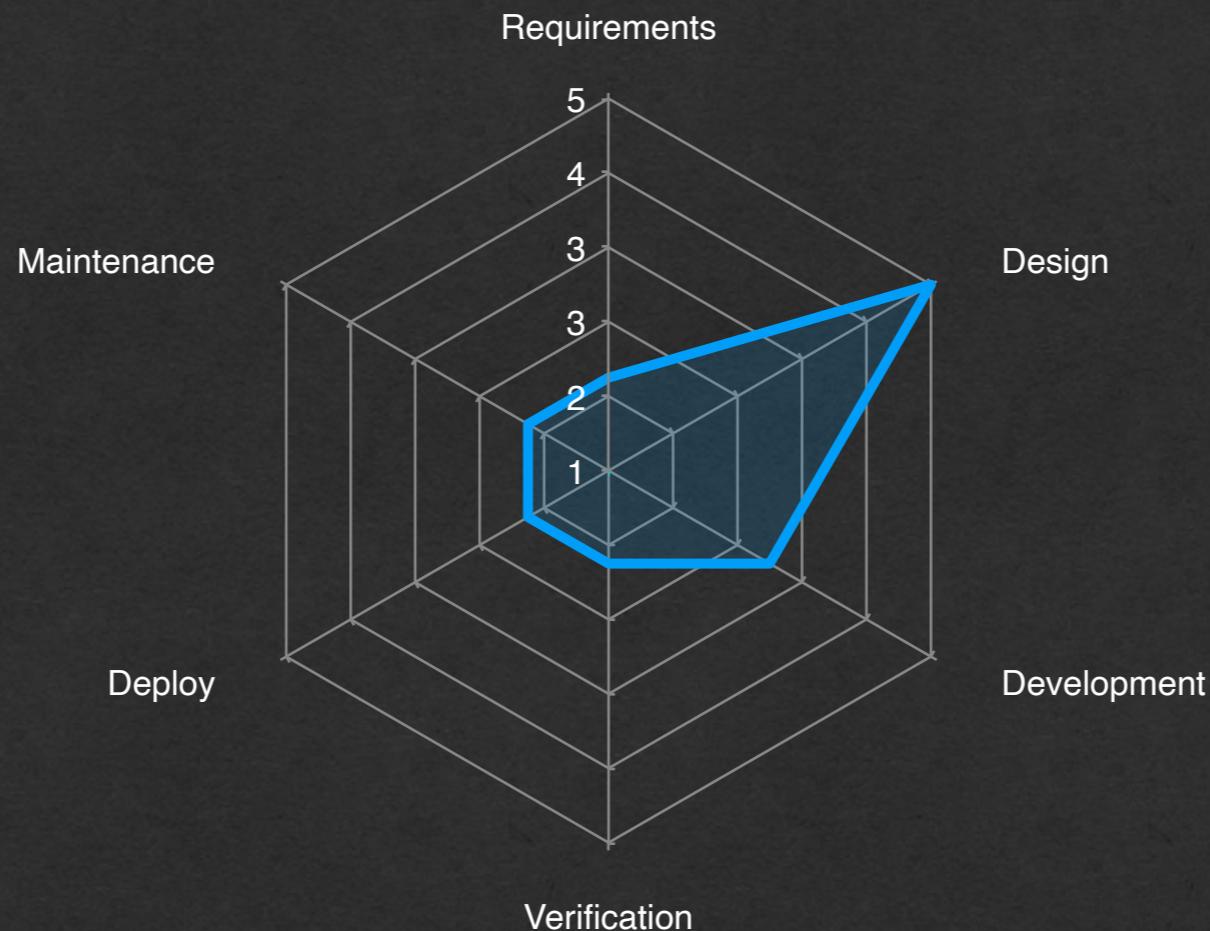
Risultati Di Ricerca

DATI SUL SECURITY TESTING I.T.SVIL



Risultati Di Ricerca

DATI SUL SECURITY TESTING I.T.SVIL

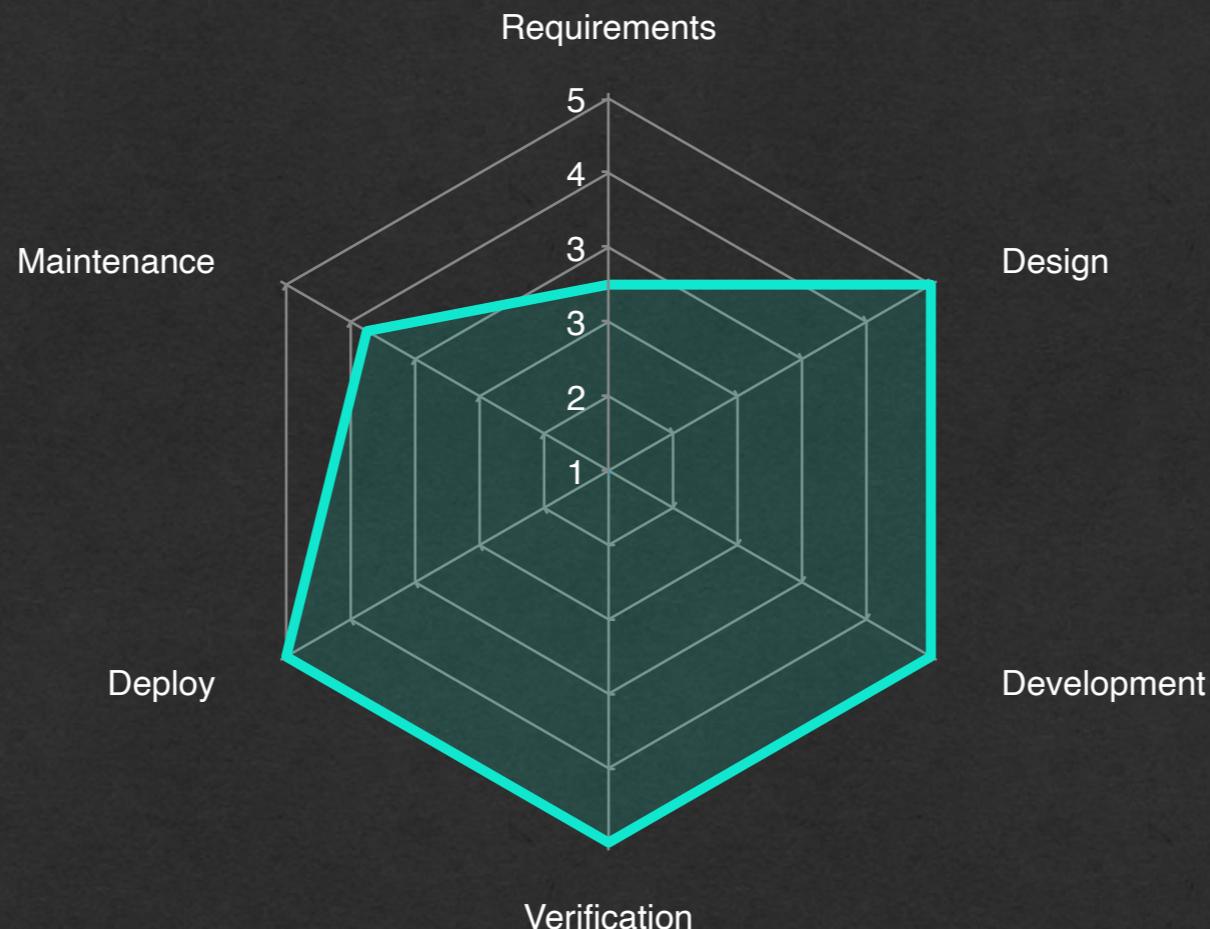


I.T.Svil non utilizza framework di sicurezza, ma applica tecniche sporadiche di security testing

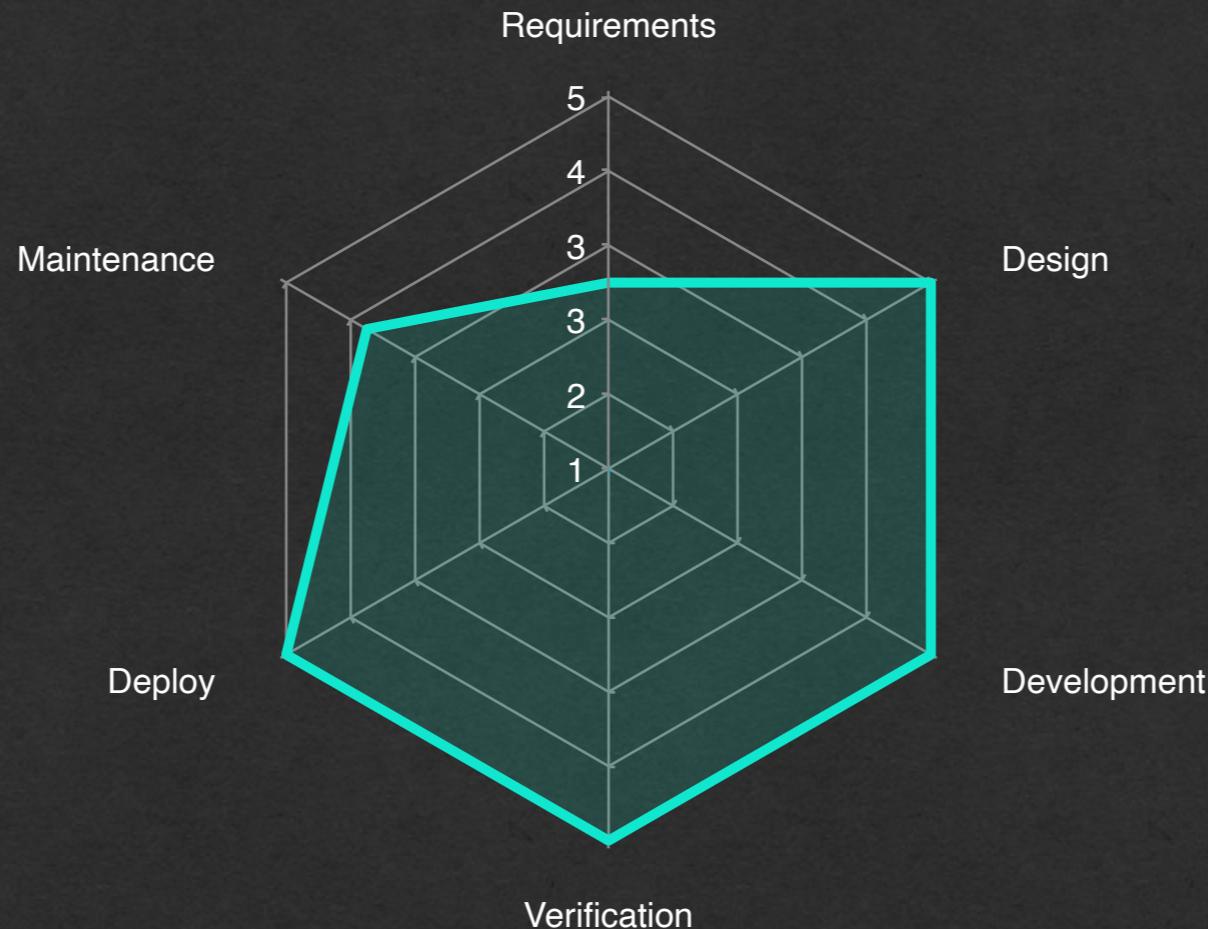


Risultati Di Ricerca

DATI SUL SECURITY TESTING SAP



DATI SUL SECURITY TESTING SAP

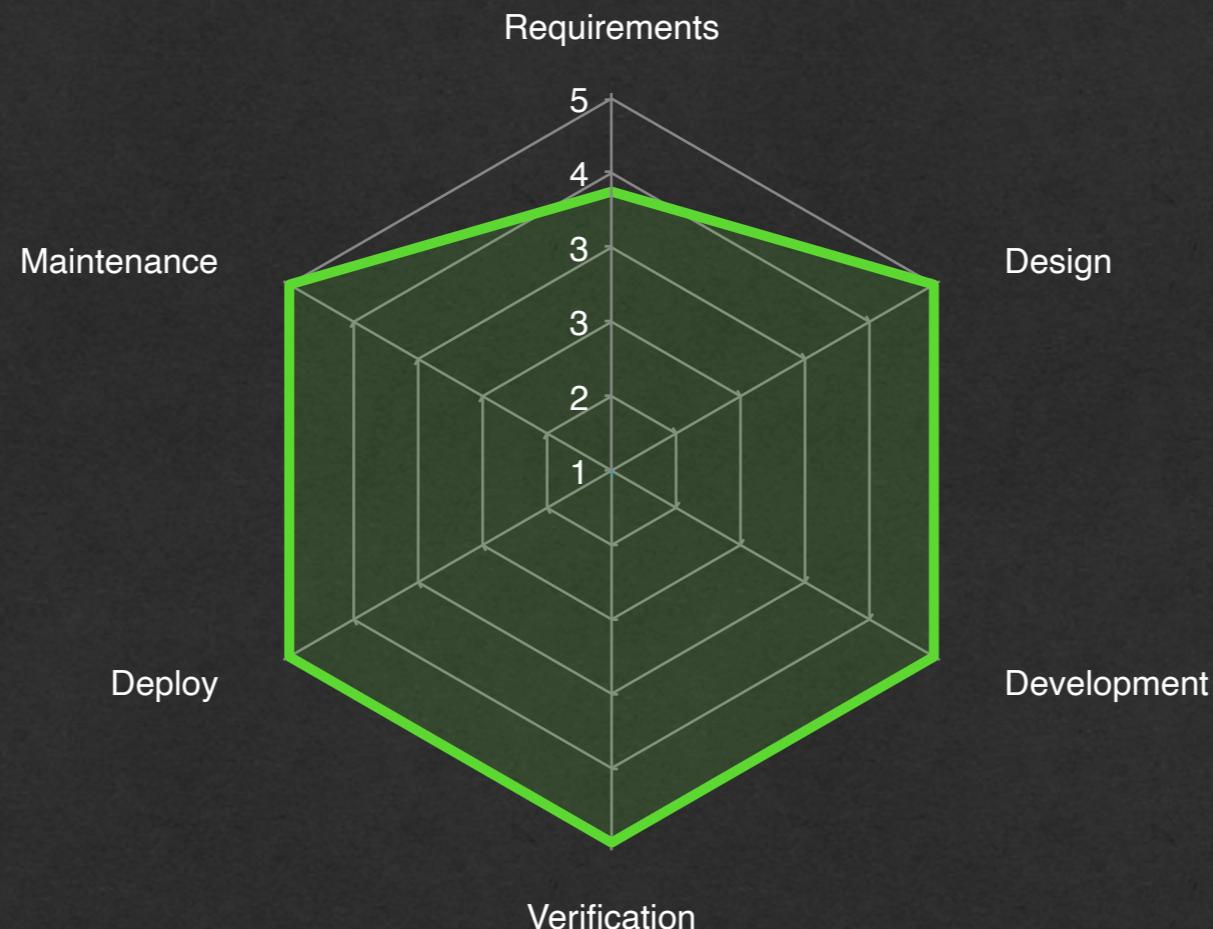


SAP utilizza framework e tecniche di security testing, facendole variare però, alla tipologia di software da sviluppare.



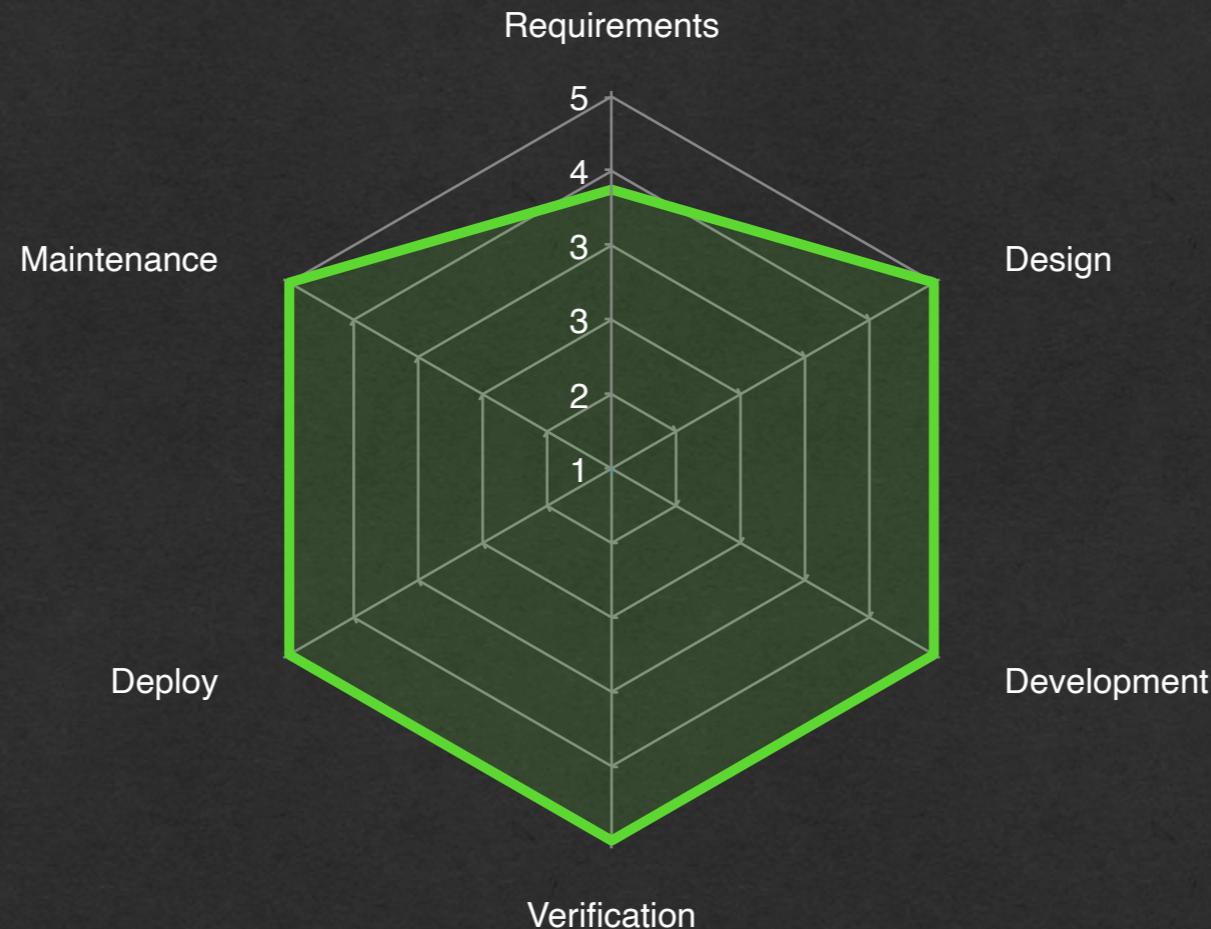
Risultati Di Ricerca

DATI SUL SECURITY TESTING ZUCCHETTI



Risultati Di Ricerca

DATI SUL SECURITY TESTING ZUCCHETTI



Anche Zucchetti utilizza i framework di sicurezza durante l'intero sviluppo... ma...



Risultati Di Ricerca

INTERVISTA INDIVIDUALE



Gregorio Piccoli, *CTO*
Zucchetti

“I framework di OWASP e Microsoft devono essere usati da persone con il giusto background tecnico. Uno sviluppatore che non conosce nulla di sicurezza, non saprebbe come utilizzarli.”



Risultati Di Ricerca

INTERVISTA INDIVIDUALE



Gregorio Piccoli, *CTO*
Zucchetti

“Ma prima di usare i framework di sicurezza per scovare gli errori, è necessario imparare a sviluppare in sicurezza.”



Risultati Di Ricerca

INTERVISTA INDIVIDUALE



Gregorio Piccoli, *CTO*
Zucchetti

“Noi di Zucchetti, abbiamo un team di Ethical Hacker che comunica continuamente con il team di sviluppo. L'intera comunicazione è gestita dai manager di sicurezza.”



Risultati Di Ricerca



Il Security Testing è un'attività che le aziende affidano a professionisti con competenze in sicurezza e non ai comuni sviluppatori.



Risultati Di Ricerca



Il Security Testing è un'attività che le aziende affidano a professionisti con competenze in sicurezza e non ai comuni sviluppatori.



Due Aziende su tre si affidano al Secure Development Lifecycle ed ai framework di sicurezza.



Risultati Di Ricerca



Il Security Testing è un'attività che le aziende affidano a professionisti con competenze in sicurezza e non ai comuni sviluppatori.



Due Aziende su tre si affidano al Secure Development Lifecycle ed ai framework di sicurezza.



L'intero processo introduce delle figure manageriali che coordinano le comunicazioni tra il team di sviluppo e il team di sicurezza.



Risultati Di Ricerca



Il Security Testing è un'attività che le aziende affidano a professionisti con competenze in sicurezza e non ai comuni sviluppatori.



Delle tre aziende analizzate, due si affidano al Secure Development Lifecycle ed ai framework di sicurezza.



L'intero processo introduce delle figure manageriali che coordinano le comunicazioni tra il team di sviluppo e il team di sicurezza.



L'intero processo è svolto da gruppi di persone. Formalmente, chiamati team di sicurezza.



Tecniche di Security Testing

Identificare le tecniche di **Security Testing** e come variano con le tipologie di **architetture** del software. Creando ulteriori linee guida per gli sviluppatori e uno standard aziendale da poter seguire.



Tecniche di Security Testing

Identificare le tecniche di **Security Testing** e come variano con le tipologie di **architetture** del software. Creando ulteriori linee guida per gli sviluppatori e uno standard aziendale da poter seguire.

Sviluppo di Tool

Creazione di **tool** per l'analisi del codice sorgente e per la predizione di codice dannoso.



Tecniche di Security Testing

Identificare le tecniche di **Security Testing** e come variano con le tipologie di **architetture** del software. Creando ulteriori linee guida per gli sviluppatori e uno standard aziendale da poter seguire.

Sviluppo di Tool

Creazione di **tool** per l'analisi del codice sorgente e per la predizione di codice dannoso.

L'unione dei due sviluppi futuri potrà creare un tool capace di suggerire – in base all'architettura e al codice sorgente – la tecnica di Security Testing più adatta.



Security Testing in the Wild: An Empirical Study into the Security Testing Methodologies in Practice

GRAZIE PER L'ATTENZIONE



Questa tesi ha contribuito a piantare un albero in Kenya



Dario Di Dario

d.didario@studenti.unisa.it 

<https://github.com/Dariucc07> 

www.linkedin.com/in/dario-di-dario 