GOVERNANCE: TRAINING		
Objective	**Activity**	**Level**
promote culture of security throughout the organization	provide awareness training	1
ensure new hires enhance culture	include security resources in onboarding	
act as informal resource to leverage teachable moments	establish SSG office hours	
create social network tied into dev	identify satellite during training	
build capabilities beyond awareness	offer role-specific advanced curriculum (tools, technology stacks, bug parade)	2
see yourself in the problem	create/use material specific to company history	
reduce impact on training targets and delivery staff	offer on-demand individual training	
educate/strengthen social network	hold satellite training/events	
align security culture with career path	reward progression through curriculum (certification or HR)	3
spread security culture to providers	provide training for vendors or outsource workers	
market security culture as differentiator	host external software security events	
keep staff up-to-date and address turnover	require annual refresher	

Figura 16 - Training practice BSIMM

Risultati più rilevanti:

Maturity Model	BSIMM2 - https://www.bsimm.com/download/

8.2 Analisi dei Processi SSDLC

8.2.1 McGraw's Secure Software Development Life Cycle Process

McGraw[30] [1] si propone di accrescere il processo SDLC (cascata o iterativo) attraverso l'integrazione di alcune attività SSD. In sostanza, il processo di McGraw si focalizza su:

- incorporazione dei requisiti di sicurezza,
- esecuzione dell'analisi dei rischi durante le diverse fasi di sviluppo,
- applicazione di metodi di security assurance quali test di sicurezza risk-based,
- analisi statica e test di penetrazione.

Il processo suggerisce anche di utilizzare l'analisi dei rischi durante la fase di progettazione. Per la fase di security assurance, McGraw suggerisce di utilizzare gli abuse cases e i requisiti di sicurezza per guidare i test di penetrazione.

[30] G. McGraw, Software Security: Building Security In, Addison Wesley, 2006