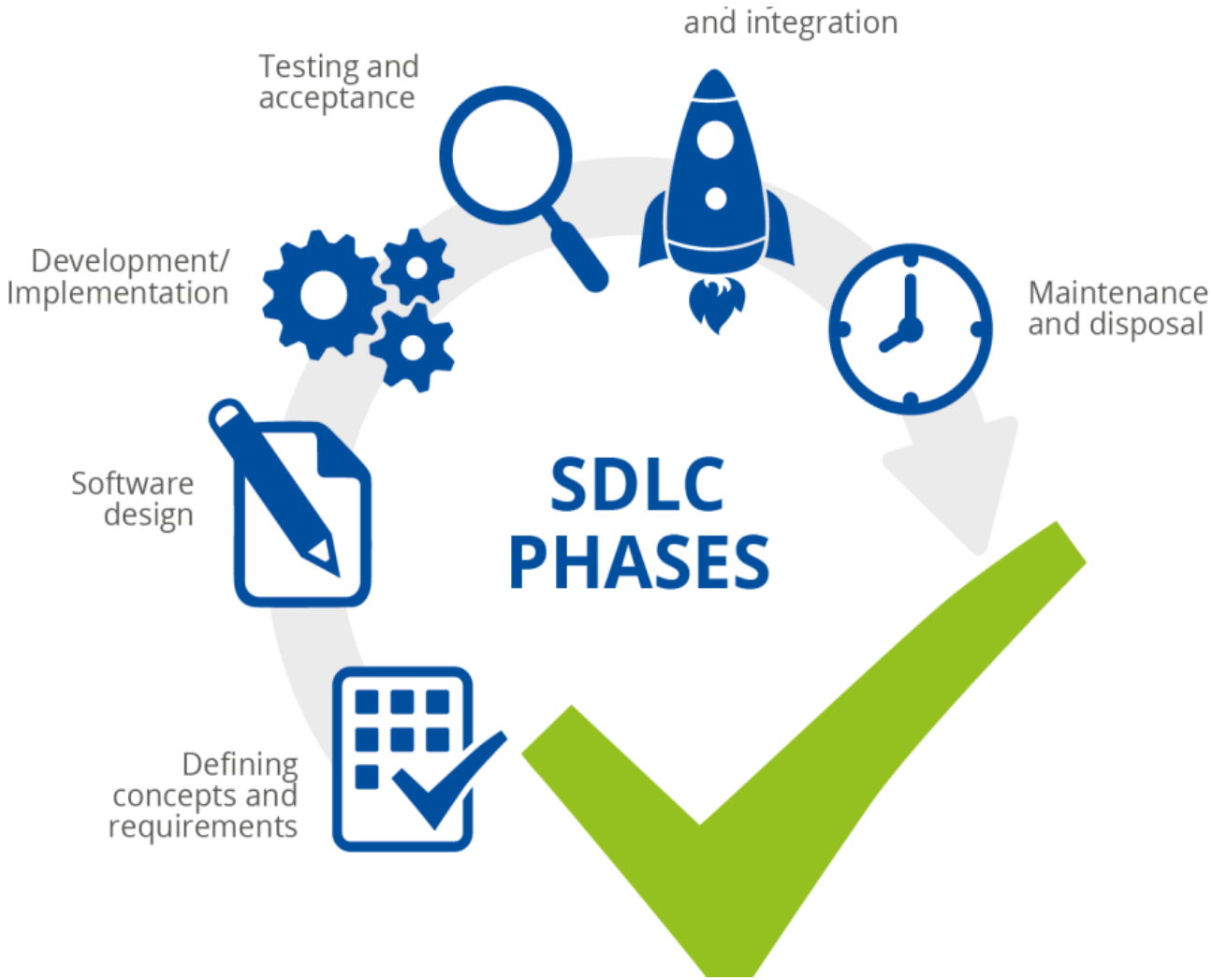
Security by design e IoT

Alberto Traballesi

Security by design e IoT (1)

- La sicurezza come base della progettazione (*Security by Design*) è l'approccio per sviluppare software sicuro per garantire la sicurezza e la privacy dei sistemi sin dall'inizio
- **ENISA** in uno studio raccomanda vivamente che la sicurezza e la privacy siano assicurate sin dalla progettazione e per impostazione predefinita.
- Lo studio ENISA identifica una serie di buone pratiche e linee guida da applicare nelle diverse fasi di progettazione del SDLC (Software Development Life Cycle) delle soluzioni IoT
- SDLC comprende le sei fasi illustrate nella slide seguente

SDLC (Software Development Life Cycle) .



Security by design e IoT (2)

- Sicurezza significa non solo costruire e distribuire software sicuro, ma anche avere un processo SDLC dell' IOT sicuro perché questo processo può essere esposto a molte minacce.
- lo studio identifica le minacce alla sicurezza che interessano il processo SDLC dell'IoT, descrive potenziali scenari di attacco e consiglia procedure e misure di sicurezza per proteggerlo
- L'IoT è fortemente legato al mondo informatico e le implicazioni di sicurezza sono significative e particolarmente rilevanti quando si progetta una soluzione IoT che, nella visione di ENISA, non include solo i dispositivi IoT, ma l'intero ecosistema che contiene anche tutto ciò che è collegato a questi dispositivi.

Security by design e IoT (3)

- L'approccio adottato dal **NIST** (National Institute of Standards and Technology) è rivolto ai produttori di apparati IoT e parte dalla constatazione che i dispositivi spesso non hanno proprie capacità per mitigare i rischi di sicurezza.
- Conseguentemente i clienti potrebbero non sapere che devono modificare i processi esistenti per accogliere l'IoT.
- il NIST invita ad analizzare il ciclo di sviluppo dei dispositivi IoT da parte del produttore e individuare quali requisiti di sicurezza devono essere considerati, implementati e documentati, nonché le implicazioni nella distribuzione dei dispositivi IoT da parte dei clienti. I produttori devono aiutare i clienti nella gestione dei rischi di sicurezza informatica valutando attentamente quali funzionalità prevedere.
- La base per gli approcci ENISA e NIST è comune ed è la *Secure by Design*. Quello di ENISA è sistemico, mentre quello del NIST è più pragmatico e focalizzato per definire le linee di base di sicurezza.

Nist divide in due fasi :

Premarket , nella quale il produttore determina i requisiti di cybersecurity in base agli utilizzi ipotizzati

Post market, nel quale il produttore comunica con gli utilizzatori dopo aver definito metodi e contenuti della comunicazione