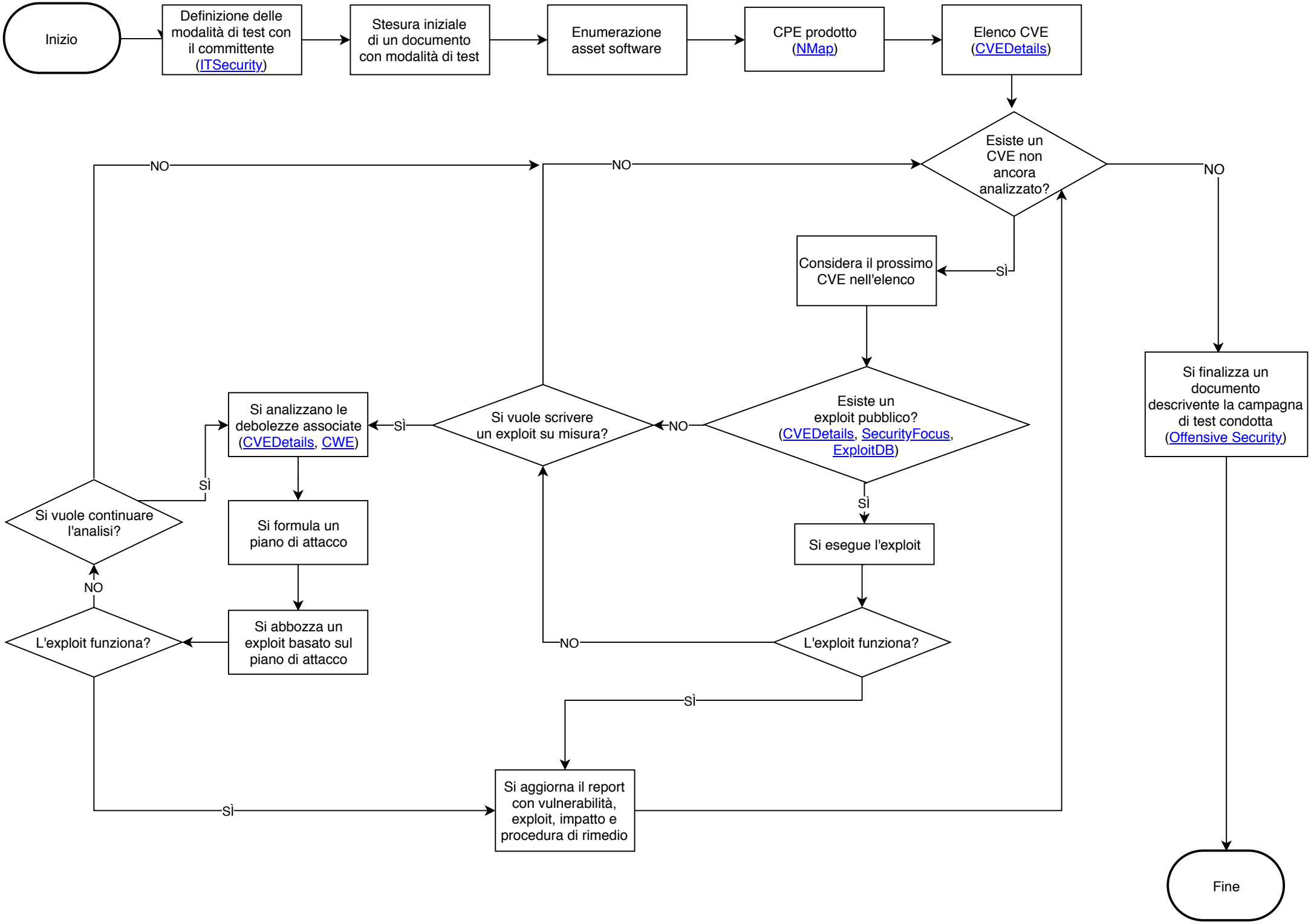
Inizio
Definizione delle modalità di test con il committente (ITSecurity)
Stesura iniziale di un documento con modalità di test
Enumerazione asset software
CPE prodotto (NMap)
Elenco CVE (CVEDetails)
Esiste un CVE non ancora analizzato?
NO
SÌ
Considera il prossimo CVE nell'elenco
Esiste un exploit pubblico? (CVEDetails, SecurityFocus, ExploitDB)
NO
SÌ
Si vuole scrivere un exploit su misura?
SÌ
Si analizzano le debolezze associate (CVEDetails, CWE)
Si formula un piano di attacco
Si abbozza un exploit basato sul piano di attacco
L'exploit funziona?
NO
Si vuole continuare l'analisi?
SÌ
NO
Si esegue l'exploit
L'exploit funziona?
NO
SÌ
Si aggiorna il report con vulnerabilità, exploit, impatto e procedura di rimedio
SÌ
Si finalizza un documento descrivente la campagna di test condotta (Offensive Security)
Fine