Adversary Simulation Readiness Checklist

Use this checklist before a scoping conversation. Mark anything unknown as **Not sure** and name who will find out.

A gap is a planning item, not a failed check. Keep system names, access details and incident information in your own approved records; general descriptions are enough here.

01 Frame the question

> We want to establish whether _____ can reach _____, and whether our defenders can detect and contain it within agreed boundaries.

YOUR VERSION

Name a business outcome, such as access to a restricted function, rather than a list of techniques.

PLANNING FIELD	YOUR NOTES
Decision this exercise should inform	
Function or boundary in scope	
Starting position: entry path tested, or access assumed	
Exclusions and stop conditions	
Target decision date	

02 Check the conditions

Record **Confirmed**, **Needs work** or **Not sure** for each.

CHECK	STATUS	OWNER OR NEXT ACTION
A sponsor agrees the purpose and how findings will be used.		
An authorised contact can approve scope, including third parties.		
Someone can pause the exercise and reach operations quickly.		
Logging and defensive visibility are understood, gaps included.		
The Control Group, who know the exercise is running, is agreed.		
Someone will own and prioritise the actions afterwards.		

03 Pick a starting point

One system or release needs an answer. Start with a targeted penetration test.

You need to see attacker reach and defensive response across a scenario. Discuss adversary simulation.

You can act on findings and want to measure improvement over repeated operations. Discuss CAOS (Continuous Adversary Operations Service).

Several answers above are unknown. Resolve those first. A narrower scenario may be the right first step.

Bring the completed checklist to a scoping conversation. It is a planning aid, not an audit or a maturity assessment.

Discuss your testing priorities

www.silentgrid.com/contact