PENETRATION TESTING

DECISION GUIDE

01 PREPARATION PHASE

PRE-TESTING

Define drivers and purpose for conducting pen test

Why do we need a penetration test?

What are we trying to accomplish with this pen test?

Produce requirements specs

What are our requirements for testing?

Identify target environments to be tested

Where do we want to focus the testing?

What assets are the most critical to protect?

Evaluate and select suitable pen testing vendor.

What is our evaluation criteria for pen test vendors?

Eg. Expertise / experience / breadth &

depth of coverage / pricing / availability

TESTING PHASE 02

Determine testing approach

Black box? White box? Grey box?

Determine type of penetration test

Network Pen Test? Application Pen Test? External? Internal?

Determine testing constraints

Are there assets or locations that must

be excluded from testing? Time restrictions?

Define scope of testing

Which assets are in-scope and which are out of scope?

Identify and Exploit vulnerabilities

How much is manual vs automated testing?

Report key findings

What type of report or deliverable will suit our needs?

Full detailed report or Exec summary, or both?

03 FOLLOW-UP PHASE

POST TESTING

Remediate vulnerabilities & weaknesses

Does the reporting prioritize remediation efforts?

Do we have resources to perform remediation?

Identify and address root causes of weaknesses

Can root causes be addressed to avoid the presence of future vulnerabilities and weaknesses?

Initiate improvement plan from lessons learned

What processes and procedures can be improved based on findings?

Evaluate the effectiveness of the pen test

Was the testing successful in meeting testing criteria and achieving testing goals?

DRUMMOND

WWW.DRUMMONDGROUP.COM

SECURITY | COMPLIANCE | PRIVACY | RISK MANAGEMENT