CHECKLIST

HALOCK® Purpose Driven Security

10 MUST-HAVE CAPABILITIES OF BEST-IN-CLASS PEN TESTING PROVIDERS

BEFORE AND DURING THE PEN TEST:

- [ ] **1. DETAILED AND ACCURATE PROJECT SCOPE**
Start with a dedicated scoping meeting to ensure the scope is defined properly and expectations are understood. The pen testing firm's team should include subject matter experts to engage with your team, fully understand your business and network environment, and properly capture your scope and requirements.

- [ ] **2. PROJECT MANAGEMENT DISCIPLINE**
A detailed project plan should be created and each penetration test should be treated as a project to ensure your expectations are met and testing can be performed under controlled conditions. Pen test projects should be managed by experienced project managers with PMI PMP certification.

- [ ] **3. DEDICATED TEAM**
A dedicated team should be assigned to each pen test project, allowing you to complete the pen test in the shortest time period feasible in order to minimize impact to your business.

- [ ] **4. INDUSTRY-STANDARD METHODOLOGY**
Beware of "proprietary" pen testing methodologies. A pen testing firm should disclose and utilize an industry-standard pen testing methodology to ensure that the pen testing results are repeatable and well understood by your auditors.

- [ ] **5. COMMUNICATION PLAN**
As part of project management practices, a communication plan should be established to define your preferred method of communication with the team, stakeholder(s) and sponsor(s). Communications between the penetration test team and your stakeholders should occur regularly to keep you aware of your project status.

- [ ] **6. COMPREHENSIVE DELIVERABLES**
A final report deliverable should not be in the form of a simple spreadsheet or lengthy email. Instead, a content-rich report with screenshots describing each exploit and step-by-step descriptions should be provided so that your team can reproduce the exploit, understand the impact, and conduct remediation.

- [ ] **7. QUALIFIED U.S. BASED ETHICAL HACKERS**
Pen testing is a process deeply personal and confidential to your business. Pen testers should be the best in their field and reside within the U.S. They should maintain appropriate certifications related to their testing specialty.

AFTER THE PEN TEST:

- [ ] **8. REMEDIATION VERIFICATION**
Following a pen testing engagement, the penetration testing firm should offer services to validate that remediation efforts were successful and vulnerabilities were resolved.

- [ ] **9. RISK ANALYSIS**
Once your pen test is complete, the Firm should be able to help your organization with the findings. Quality firms will have the capability to analyze findings and prioritize them by risk and offer to prepare executive-level reporting. Choose an information security firm with a strong competency in Governance, Risk and Compliance to support you in incorporating the pen test results into your risk assessment risk register. If you don't have a risk register, they should be able to help you establish a risk management framework appropriate for your business.

- [ ] **10. VULNERABILITY REMEDIATION**
Once your pen test is complete, your pen test provider should have the capabilities to assist your organization post-assessment. They should have the ability to build remediation plans, validate remediation designs, and assist with implementing fixes.

847.221.0200 NON EMERGENCY
800.925.0559 EMERGENCY RESPONSE HOTLINE
www.halock.com
info@halock.com