



EXCEEDING EXPECTATIONS.

## A Disciplined Approach

Implementing and maintaining security controls is a complex effort. How does the organization know the investment and effort has produced the desired results?

Conducting a penetration test is the most effective method to evaluate their effectiveness. A penetration test involves techniques used by a real attacker but must be performed under safe and controlled conditions. The most common questions asked when preparing for a penetration test relate to knowing what to expect. HALOCK is very different in this regard.

Collaboration begins well before the first test is run and continues throughout the process. HALOCK conducts penetration testing **with you**, not to you. HALOCK utilizes a repeatable and closely managed process on every single penetration test project to ensure you know **exactly what to expect**. This begins with scope definition, progresses through detailed planning, execution, delivery of results, and post assessment.

## Project Progression

1

SCOPE  
DEFINITION

2

PLANNING  
AND  
PREPARATION

3

PENETRATION  
TEST  
FIELDWORK

4

DELIVERY OF  
RESULTS

5

POST  
ASSESSMENT  
ACTIVITIES

# THE HALOCK EXPERIENCE

## Scope Definition

**Scope definition is as much about providing guidance and education as it is about gathering requirements.** Prior to performing any penetration test, scope definition is conducted. This collaborative session defines the goals, objectives, and expectations for the engagement and aligns the most appropriate scope, approach, methodology, and resources to ensure those expectations are met. During scope definition, HALOCK guides the discussion to obtain an understanding of your goals and objectives, advise the most appropriate methodologies to utilize for your penetration test, understand technical or budgetary constraints, and provide education and guidance. Following this session, HALOCK produces your first deliverable\*, a detailed statement of work. This document details the objectives of the test, the methodologies and tests to be performed, the project management framework and approach, defined customized scope and boundaries for the engagement, fees and payment terms, assumptions, terms and conditions, sample deliverables, and supplemental content. This document is reviewed with your organization to answer any additional questions you may have, make revisions when applicable, and confirm that the documented approach accurately and concisely reflects the expectations of all stakeholders.

## Planning and Preparation

Proper planning is critical to ensure testing is performed in a quality manner and under safe and controlled conditions. Initiation triggers planning and preparation with key stakeholders. This process, led by a HALOCK subject matter expert, involves conducting one or more interactive planning sessions to gather the information needed to develop the detailed project plan. Any necessary preparation tasks, required documentation, communication with key stakeholders, scheduling considerations, and logistics are discussed. HALOCK produces your second key deliverable\* during this phase, the project plan. The project plan details the complete timeline of events, technical considerations, communication, and ultimately ensures that all parties are well prepared and **know exactly what to expect** throughout the process. As the scheduled fieldwork dates approach, reminders and other relevant communication occurs.

## Penetration Test Fieldwork

With the project plan in hand as the playbook, testing begins. HALOCK issues notifications throughout the process to ensure interested parties are reminded and updated of key activities as they progress. HALOCK progresses through the scope of review as defined in the plan, evaluating each vulnerability identified, and pursuing exploits to demonstrate impact. Communication of key milestones or critical issues occurs throughout testing. Very little support is needed from your team at this stage as HALOCK is equipped with all that is needed in the project plan. Quality assurance activities are also conducted throughout testing to ensure objectives are being met, testing efforts are completed as expected, and that all necessary evidence has been gathered. As fieldwork activities are completed, HALOCK incrementally documents vulnerabilities observed, visual demonstrations of exploits, develops recommendations, and completes any necessary supporting information. This ensures the team will have all the necessary information to develop the formal report and can do so in an expedited fashion. The team progresses through each area of the scope of review as documented in the plan. When testing concludes, an all stop notification is issued and the team transitions to reporting. The reporting phase involves compiling all findings and evidence into the detailed report, document recommendations, and issue the report to the QA process.

## Delivery of Results

Every report written is subjected to HALOCK's stringent QA standards. This process ensures every finding is well documented, clearly articulated, and is accompanied by meaningful and actionable recommendations. The detailed report, your third deliverable\*, is then issued to your designated project sponsor to review internally. A collaborative review meeting is also coordinated by HALOCK as a follow up. This review session is an open agenda with the participants you wish to include in the discussion such as information security staff, information technology resources, auditors, or members of management. During this session, topics such as remediation considerations are discussed, questions your team may have are answered, key findings are reviewed, and next steps such as upcoming planned activities are coordinated.

## Post Assessment Activities

Post assessment marks the end of the penetration test and the beginning of remediation. Quite a bit has been completed to reach this stage, but there are almost always planned activities that follow. These activities vary greatly based on the vulnerabilities identified during testing, the role of the penetration test in your broader security management program, and other considerations. While the penetration test may be complete, **HALOCK is here to support you.** This support can include ongoing counseling and advisory, presenting to your executive audiences, remediation assistance, risk management support, and conducting follow-up remediation verification tests.

\*Samples available