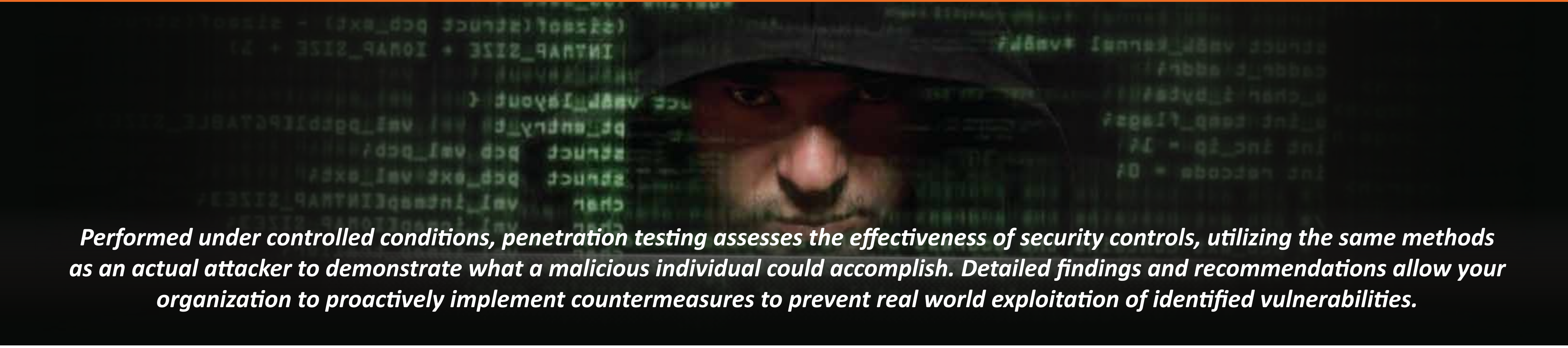
PENETRATION TESTING



Performed under controlled conditions, penetration testing assesses the effectiveness of security controls, utilizing the same methods as an actual attacker to demonstrate what a malicious individual could accomplish. Detailed findings and recommendations allow your organization to proactively implement countermeasures to prevent real world exploitation of identified vulnerabilities.

What are my scope options?

External Network Penetration Tests differ from automated vulnerability scans in that efforts are focused on actually exploiting weaknesses with the intent of gaining access to the environment. They are performed remote to the environment to target internet facing networks, hosts, and services.

Internal Network Penetration Tests are performed internal to the environment to focus on private hosts behind the perimeter firewalls. Internal penetration tests begin with unauthenticated access and leverage vulnerabilities that would allow an attacker to gain privileged access to protected information and systems.

Web Application Penetration Tests provide a flexible framework for comprehensively identifying and evaluating vulnerabilities specific to web application coding weaknesses. Testing is typically performed with prior knowledge to ensure a deep understanding of the purpose of the application and utilize a variety of scenarios specific to the end users of the web application.

Wireless Penetration Tests assess the adequacy of security controls designed to protect unauthorized access to wireless services. Attempts to exploit wireless vulnerabilities are conducted to gain access to private wireless networks and escalate privileges from guest wireless access to the private network.

Onsite Social Engineering is performed to assess the effectiveness of physical security controls, employee response to suspicious behavior, and validate that network security controls cannot be bypassed by establishing an onsite presence.

Remote Social Engineering is a remote assessment performed under controlled conditions designed to validate the effectiveness of user security awareness and incident response processes. Testing includes leveraging a carefully crafted fictitious "malicious" website, email campaigns to targeted employees, phone contact, or through other customized attack scenarios.

HALOCK's Penetration Testing Team has conducted thousands of penetration tests for mid-size companies to Fortune 100 Corporations, building a solid reputation of excellence along the way. Specialized training, industry credentials, compliance and regulatory experience, and a robust support team ensures each engagement is properly scoped, expertly delivered, and addresses your specific needs.

HALOCK®
Purpose Driven Security

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

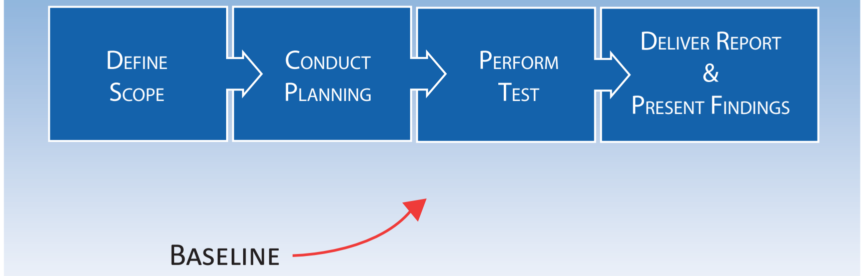
Inc. 5000

BBB ACCREDITED BUSINESS

WHAT ARE MY PROGRAM OPTIONS?

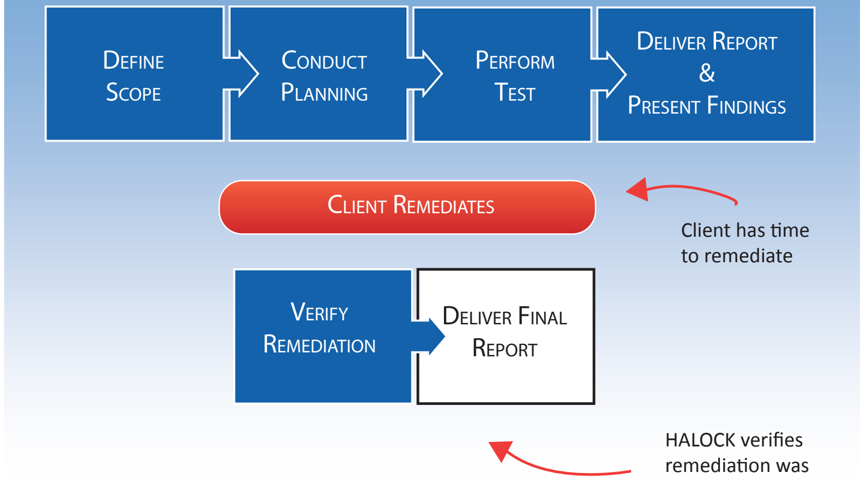
Point in Time

A point in time penetration test provides a current view of the environment. This is ideally performed folllowing a major change, when acquiring a subsidiary, or as the first penetration test performed.



Point in Time with Remediation Verification

This is the ideal approach when verification of remediation is required.

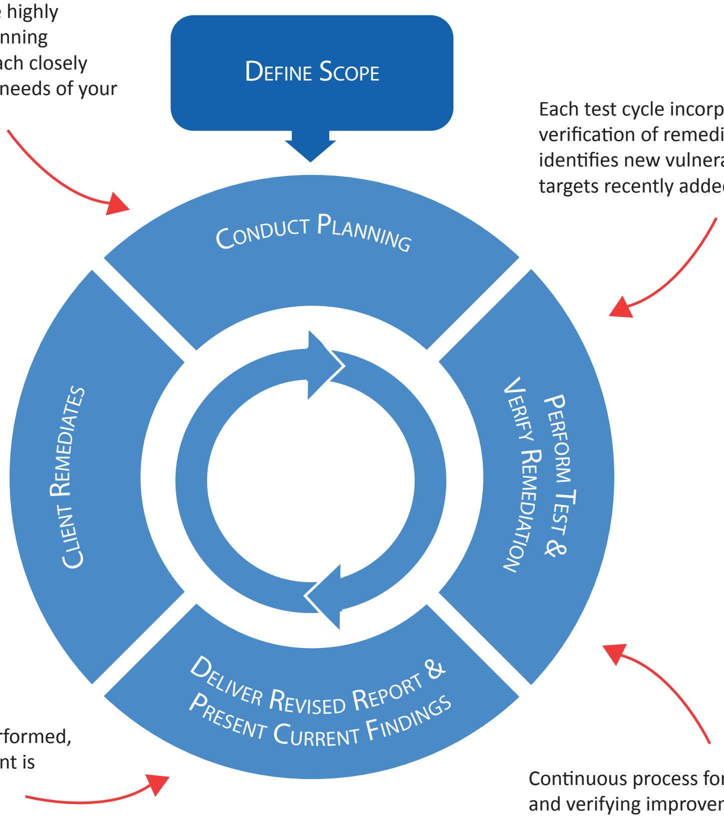


Client has time to remediate

HALOCK verifies remediation was successful

Recurring Program

Performing recurring testing narrows the window for zero day vulnerabilities and minimizes exposure for known vulnerabilities. This approach ensures vulnerabilities are identified, remediated, and verified during each test cycle. This allows you to proactively manage emerging threats over time and demonstrate improvement.


Define Scope
Conduct Planning
Perform Test & Verify Remediation
Deliver Revised Report & Present Current Findings
Client Remediates

Recurring programs are highly adaptable. Ongoing planning ensures the test approach closely aligns with the current needs of your organization.

Each test cycle incorporates verification of remediation efforts, identifies new vulnerabilities, and targets recently added hosts.

As each test cycle is performed, continuous improvement is demonstrated.

Continuous process for remediation and verifying improvement.