OnDefend

CYBER SECURITY REALIZED

Attack Simulation Testing Info Guide

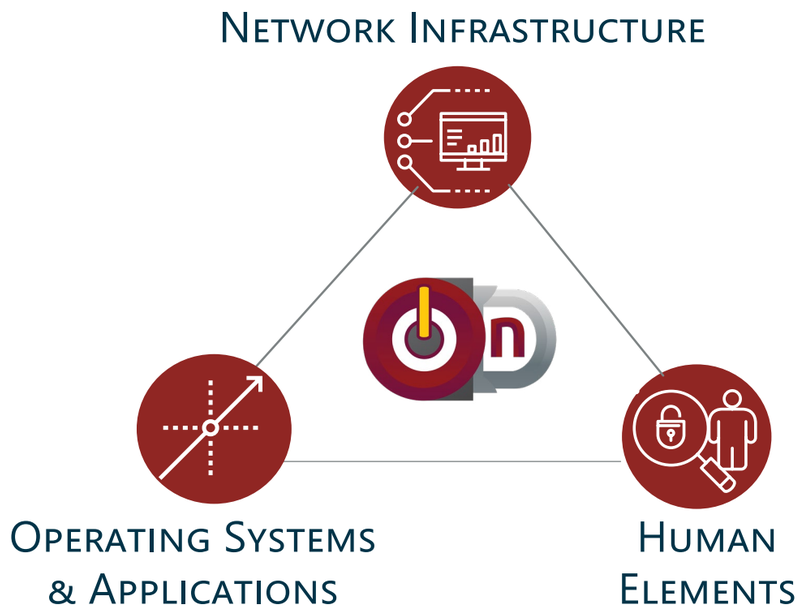
ONDEFEND.COM

WELCOME TO ONDEFEND'S TESTING SERVICES

Our testing services are built from the ground up to provide industry leading assessments based on best practices and mature frameworks. The value of any security assessment is in the actionable information to fix the problems identified in the report of findings. OnDefend's mission is to help organizations of all sizes, budgets and other factors that impact their security decisions.

Our Holistic Approach

Each service offering provides different perspectives into the security posture of an organization, with a focus on testing all layers of the technology (and people) stack in an understandable way that focuses on the true risks facing your organization.



A Snapshot In Time

Security tests are a snapshot which provide detailed information on what an attacker can do once they take advantage of that first vulnerability. Enterprises are like living things, always changing as new systems come online, upgrades to applications are made, infrastructure changes are made to accommodate business needs, and patches are released. New vulnerabilities are announced every day, meaning that a system that is fully patched and secure today may not be tomorrow. As such, security testing needs to be a continuous process, not just a single effort completed every once in a while.

OnDefend works with your organization to understand your maturity in the security testing space and builds a testing plan that meets a cadence your organization can support. This ensures you receive a frequency of testing to provide valuable data while providing enough time for remediation activities in between testing engagements.

ATTACK SIMULATION TESTING

Overview

This testing simulates the type of attacks a determined adversary might execute against our clients. This attack is focused on testing not just the information systems that make up our client's network, but also the ability of the client's security team to detect and identify these activities.

Throughout the engagement, OnDefend testers focus on mapping attack scenarios and executing the attacks while avoiding detection. Each phase builds on the previous phases, although additional equipment may be provided to ensure a more thorough test in the time windows for the project.

This type of testing is critical to understanding the resiliency of your security program to defend against this type of attack, of your security team's ability to detect and stop the attack in progress and understand where gaps and blind spots exist within the network.

Attack Simulations extend the traditional penetration test by assessing not just the security of the infrastructure, but the ability of your security team to identify and contain an active attack in the network. This provides your team with the opportunity to practice threat hunting and incident response techniques against

Methodology

a live (and trustworthy!) adversary. Often these engagements uncover gaps in the deployment of security controls as well as highlight where future training efforts can be applied. Overall, the testing teams use the Penetration Testing Execution Standard (PTES) framework when conducting these types of assessments.

Attack Simulation Testing Phases

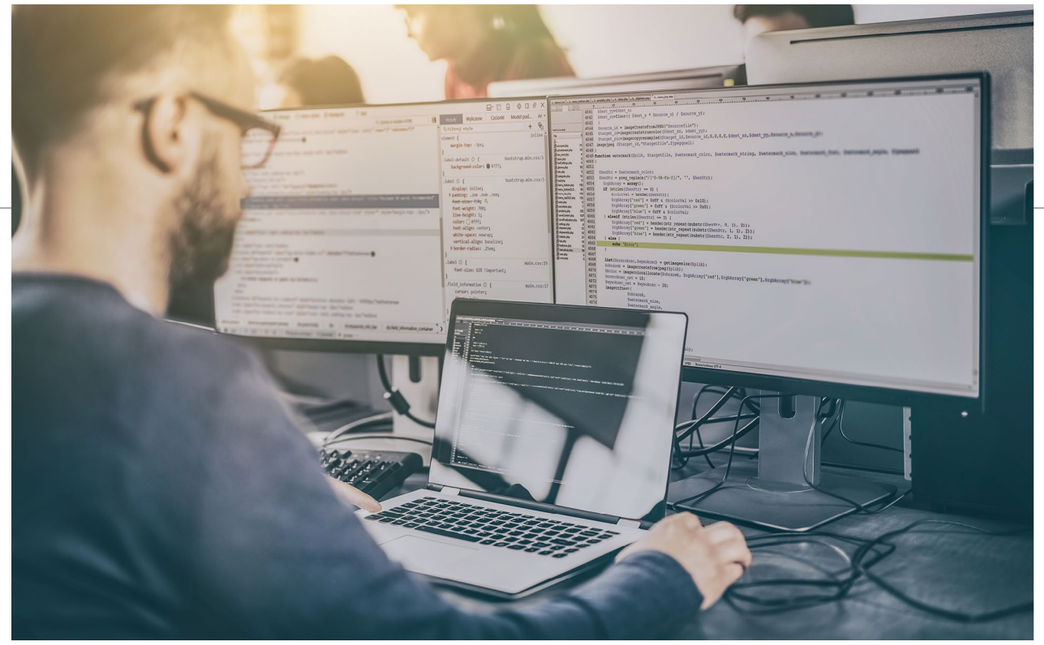
1. External Network Review
2. Internal Network Testing
   - Mapping & Reconnaissance
   - Service Identification
   - Vulnerability Analysis
   - Exploitation
   - Post Exploitation
3. Data Exfiltration Testing
4. Analysis & Reporting

ATTACK SIMULATION TESTING

1. External Network Review

Internet facing systems are under constant attack from all corners and ensuring the security posture is an important first step in the engagement. A compromised system here would give an attacker a foothold in your organization. OnDefend testers will focus on identifying possible vulnerabilities that would enable an attacker to gain system and network access during this phase.

Understanding what is observable from the Internet from an adversary perspective is a vital component of protecting those perimeter systems.



2. Internal Network Testing

EXAMPLE SCENARIO: COMPROMISED HOST SIMULATION

While information security traditionally provides the majority of its protective and detective power at the network perimeter, a compromised workstation is a common event. This phase of testing simulates how an adversary would move through a network from the inside, whether from a system compromised by an external network attack, a successful phishing email, or physical access gained on the network.

OnDefend will provide a compact remote Sentinel testing platform to conduct covert testing operations within your network. OnDefend testers look to achieve their access goals while avoiding detection by your security team.

OnDefend
CYBER SECURITY REALIZED

ATTACK SIMULATION TESTING

3. Data Exfiltration Testing

Organizations that maintain sensitive data often invest resources in various methods to ensure that the sensitive data does not leave the network without permission. In this phase, OnDefend testers will build on the work of the previous testing activities to identify the different methods to successfully transmit your provided test data out of the network. OnDefend testers will leverage several different techniques and tactics to provide your security team a realistic simulation to ensure that the data loss prevention mechanisms in place are working as expected.

4. Analysis & Reporting

All exploitable security vulnerabilities in the target system are recorded and associated risk-based severity scores are reported to the client. The identified security vulnerability is thoroughly assessed and reported along with appropriate recommendation or mitigation measures.

OnDefend
CYBER SECURITY REALIZED

Test reports include:

- Details on how each finding was identified and confirmed
- Severity rankings
- Effective remediation recommendations
- Full narrative of the engagement
- Detailed recommendations of additional detection strategies
- Identifying the effective controls that prevented various attacks from working

Client may request results in alternative formats to facilitate importing into GRC tool or ticketing system as necessary. See Sample Test Report to view our test results deliverable.

Tools and Techniques

OnDefend testers focus on the fundamentals of the systems and applications that are being tested, rather than focusing on specific software testing tools. This adaptive approach enables OnDefend testers to leverage commercial products, open source tools, and custom developed scripts and applications to conduct testing. OnDefend consultants are constantly learning and teaching new skills and techniques and contribute to open source projects in the information security ecosystem.

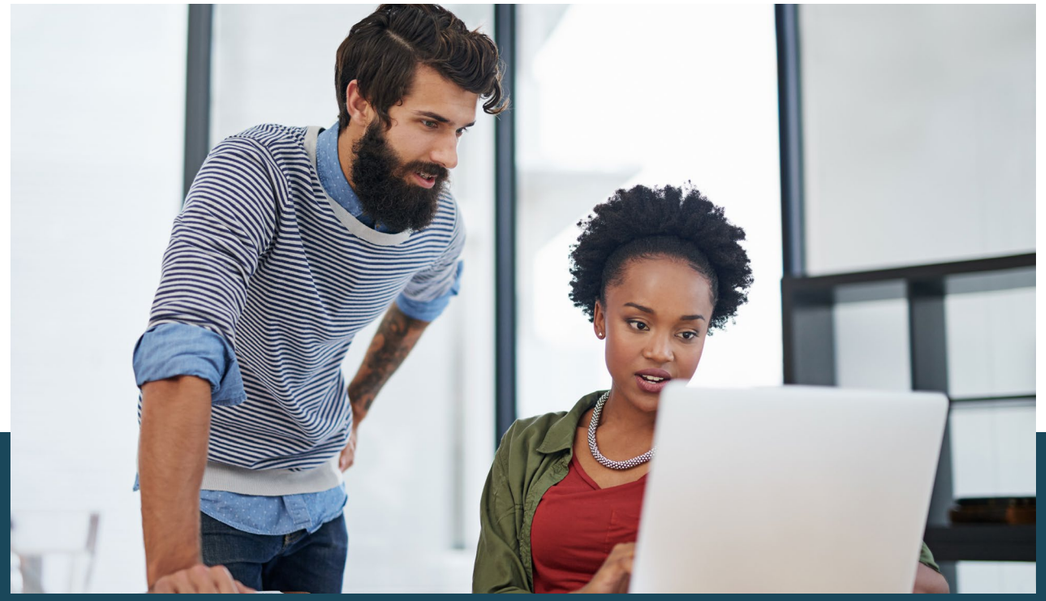
BLUE TEAM WORKSHOPS

Overview

OnDefend also provides optional Blue Team workshops as part of these engagements. In these workshops, OnDefend security testers conduct in-depth technical training, based on feedback from the customer after the report draft is delivered. OnDefend consultants tailor the workshop based on customer feedback.

The Workshop

Sometimes these courses are focused on teaching the methods used during an engagement to enable a customer's team to reproduce the findings in the report. Other sessions are built to teach tactical and strategic actions to reduce the exposure of those specific findings, or help with other security related concerns, such as incident response planning and reviews. This workshop is typically a one-day course, usually 3-4 hours of content, for up to 10 members of the customer's team.



OnDefend
CYBER SECURITY REALIZED

THE ONDEFEND TESTING TEAM

OnDefend's testing services are only as good as the talented testers we utilize to provide these services. As such, we spend significant time and resources ensuring our testers meet our standard and are constantly improving their skills and expanding their knowledge.

Qualification Program

PRACTICE ASSESSMENT

This real-world work sample method lets us see what a tester will be able to provide for our customer, not just what trivia questions he or she could answer in an interview.

PEER REVIEW

A successful outcome in the practice assessment moves the candidate along to the final interview with some of the senior team members.

EXTENSIVE BACKGROUND CHECK

OnDefend testers must pass an extensive background check in order to be hired.

SHADOW AND RECERTIFICATION

Once hired, the tester shadows other senior testers for a few engagements. All testers undergo annual recertification reviewed by our Principal Consultants.

Testing Team Credentials

OnDefend's typical tester candidate requirements:

- At least 7 years of direct security assessment experience
- A bachelor's degree in Computer Science or Software Development or comparable work experience
- Hold certifications like the EC-Council Certified Ethical Hacker (CEH) and Offensive Security Certified Professional (OSCP)
- Active members of their local information security community
- Present at various conferences and events on security related topics
- Participate in vulnerability research contests and bug bounty programs, to further develop their skills and broaden their experiences

OnDefend provides advanced training for all testers, and such training is an integral component of the employee review process. We host internal training sessions where team members share knowledge and techniques, and also sponsor "hackathons" where testers get the opportunity to work exclusively on solving a problem to make them more effective, whether building a new tool, integrating new methods into the process, or extending the platform to improve the effectiveness of our services. These events often generate ideas that we bring into production as part of the formal process, and ensure our processes and tools are driven by the quality of the testing they enable.

OnDefend
CYBER SECURITY REALIZED

OnDefend
CYBER SECURITY REALIZED

Contact Us Today

Industry Leading Professionals are here to answer any questions you may have regarding our cyber security services & solutions.

Visit us at:

OnDefend.com

Or contact us via:

Email: contact@ondefend.com

Call: 904.248.4699