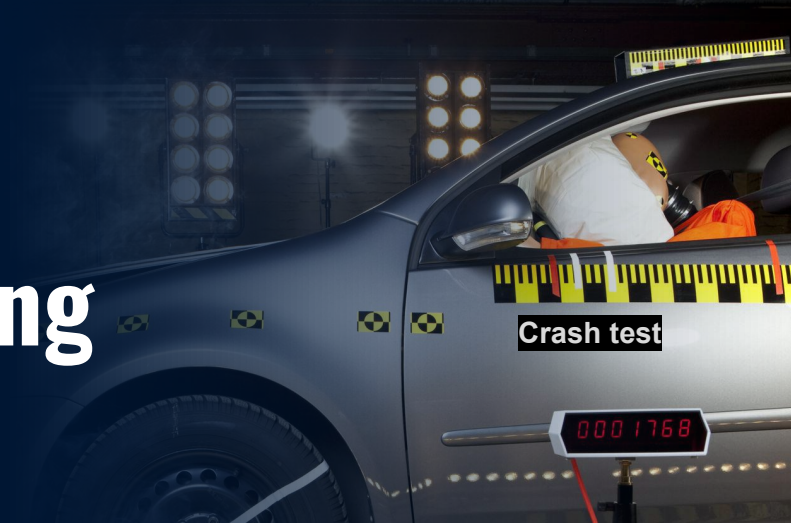
UnderDefense

Penetration Testing

Best Crash Test for your Business



BENEFITS

- Justify your security investments in security personnel & technology by providing evidence to C-level management, investors, and the board
- Stay ahead of the hacker. Identify and mitigate complex security vulnerabilities before a malefactor exploits them
- Discover flaws that may violate compliance provisions or regulations. Get a report with tactical and strategic recommendations to harden your security posture
- Know whether your critical assets are at risk. Assess the magnitude of potential business and operational impacts of successful attacks

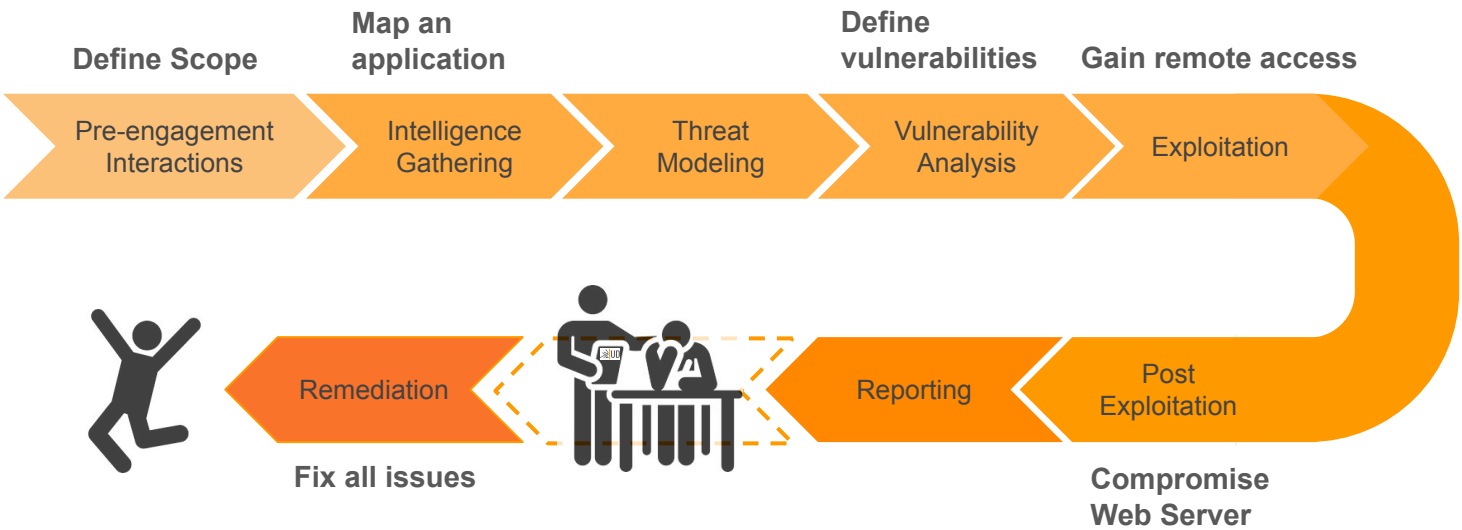
Why UnderDefense

UnderDefense is a globally top-ranked cybersecurity firm by Gartner and Clutch with elite team of certified security experts (OSCP, OSCE, CEH, CCNE, MCP, GIAC). We perform real-world attack simulations to test defenses and uncover actual risk from the perspective of a motivated attacker.
UnderDefense uses real attack knowledge, gained from Incident Response Engagements of advanced persistent threats (APTs) and attacker behavior. Our Ethical hackers use the same techniques, tactiques and procedures (TTPs) that an adversaries would use to penetrate a client's environment and disrupt business operations.

Reduce your security risks

During the pentest, security experts of UnderDefense always apply an individual approach to the needs of the client and an organization's environment. We assess the existing security program and the state of security of an organization's critical systems, networks, and applications. UD penetration testers are highly educated ethical hackers, who understand malefactors` actions, are always aware of industry trends, and leverage various attacks vectors.

Approach



Range of customizable penetration testing services

Penetration Test	Objective	Benefit
External Penetration Tests	The assessment of the internet-facing systems to determine if there are exploitable vulnerabilities or misconfigurations that expose data or allow unauthorized access	Shows the real impact of risks came from the Internet. Helps to meet all compliance requirements Identifies new exposures Justify your security investments (ROI).
Internal Penetration Tests	The assessment of organization's internal systems and applications to determine how an attacker could move laterally throughout the network and how deep the attacker or the malicious insider can reach. Test data exfiltration and MITRE coverage of your SOC/MDR	Shows the impact of compromised endpoints. Simulated real Attack-Defense exercise which allows to prepare internal IT team or test your MSSP in identifying and reacting on real cyber attacks. Demonstration of risks to C-level on practice
Web Application Assessments	Testing for possible data leakage points and vulnerabilities according to OWASP top 10. Checking if source code, API is written according to best practices and customer data is safe. Test your WAF solution	Show the actual security of the application. Crash and Load testing your application before hackers get interested in your product
Mobile Application Assessments	Testing for platform-specific vulnerabilities. An application security audit inside Android/iOS environment Validate API and code-obfuscation	Avoid fraud and manipulations from unethical consumers & identify clients at risk
Social Engineering	A set of methods for making employees take actions to allow ethical hackers to get into the organization through remote access and lateral movement to simulate data exfiltration. Includes phishing company, malware development	Test your Security Awareness program in action. Shows the awareness level of employees of cybersecurity.
Internet of Things (IoT)/Embedded Device Security Assessments	Security assessment of the device by attempting to exploit the embedded firmware, control the device by passing or injecting unsolicited malicious commands, or modify data sent from the device.	Ensure new or existing IoT systems are safe to be used in your controlled environment. Meeting regulatory requirements for IoT. Ensure the commands and information received from the device are legitimate.

WHAT YOU GET

- Report for C-level executives and board of detected vulnerabilities and business impact
- Detailed technical report with all evidence and artifacts, including videos and screenshots that have enough information to recreate our findings with IT and Development teams
- Letter of Attestation for your customers and compliance requirements
- Listing in "Certified Applications & Organizations Directory"
- 1-day free Remediation assessment to get a clean report and confirm that all defects were fixed
- Fact-based risk analysis to confirm whether a critical finding is relevant to the targeted environment
- Actionable deliverables and tactical recommendations for immediate improvement
- Mature your security strategy with recommendations for longer-term cyber resiliency hardening

Hong Kong & Macau
Tel : (852) 2893 8860
Email : sales@version-2.com.hk

Taiwan
Tel : (886) 02 7722 6899
Email : sales@version-2.com.tw

Singapore, Malaysia & SEA
Tel : (65) 6296 4268
Email : sales@version-2.com.sg