



K7 RED TEAM ASSESSMENT

Offensive Cybersecurity Evaluation to Improve
Enterprise Cyber Defences

www.k7cybersecurity.com

Is Enterprise Cybersecurity Good Enough?

Businesses are responding to the increase in cyberattacks and compliance obligations by investing heavily in enterprise cybersecurity solutions, but are unaware if their cyber defences are sufficient for their operations. Investment in cybersecurity can be justified only if the deployed solutions can repel a cyberattack from a resourceful and determined adversary, but cybersecurity leaders cannot wait for a successful cyberattack to determine where they need to improve their cyber defences.

K7 Red Team Assessment – Enterprise Cybersecurity Evaluation through Attack Simulation

The K7 Red Team Assessment simulates real-world cyberattacks to identify vulnerabilities in an organisation's internal and external cybersecurity posture and evaluate the organisation's ability to detect, respond to, and contain threats.

Without violating legal and ethical norms, K7's expert team will launch a simulated cyber offensive against the organisation based on predefined Rules of Engagement utilising the Tactics, Techniques, and Procedures (TTPs) used by threat actors to test the business's cyber defences against real-world cyberattacks.



K7 Red Team Assessment is More than a Technical Evaluation

Conventional cybersecurity assessments are restricted to evaluating the technical aspects of cybersecurity related to specific systems within an organisation, limiting the effectiveness of such exercises. The K7 Red Team Assessment provides a comprehensive evaluation of People, Process, and Technology across the enterprise, ensuring that any gap in security anywhere in the organisation can be identified and closed.

Framework

External Assessment

Identification of vulnerabilities in publicly accessible systems

Susceptibility Simulation

Testing human susceptibility to social engineering

Internal Assessment

Identifying security gaps in internal infrastructure

Components



Reconnaissance

- Open-Source Intelligence (OSINT)
- Network Scanning
- Social Engineering



Vulnerability Discovery

- Web Application Penetration Testing
- Exploiting Network Vulnerabilities
- Physical Security Testing



Vulnerability Exploitation

- Privilege Escalation
- Lateral Movement
- Maintaining Access



Probing

- Mapping Network Resources
- Identifying Sensitive Data
- Understanding Security Controls



Exfiltration

- Transferring Data
- Data Encryption
- Covering Tracks

What We Deliver

The K7 Red Team Assessment mimics the approach followed by threat actors and delivers recommendations to mitigate vulnerabilities based on the K7 team's extensive experience in securing the operations of businesses that are particularly targeted by cyber adversaries.



Vulnerabilities Discovered

Identified vulnerabilities and their potential business impact, with CVSS score, CWE ID, and OWASP category



Exploitation Techniques

How vulnerabilities were exploited and the tools used, with purpose, target system, and impact



Recommendations

Steps to mitigate deficiencies and improve security posture, with immediate reporting of imminent threats



Lessons Learned

Insight that can be applied to future security efforts, with technical and executive debriefs

Guardrails

The K7 Red Team Assessment is an aggressive exercise that stress tests the enterprise's cyber defences. Rules of Engagement will be agreed upon with technical and management teams to create a consensus-based approach to achieving the objectives of the assessment, which will include

- ▶ Zero-risk/restoration assurance
- ▶ Handling of sensitive/critical data and servers
- ▶ Ensuring business continuity is maintained and operational impact is minimised
- ▶ Data handling and confidentiality
- ▶ Testing of physical security controls



The K7 Advantage



30+ Years' Experience in Cybersecurity

K7 was founded in 1991 as a pure play cybersecurity provider. K7 now protects more than 25 million users across 27 countries and has the extensive breadth and depth of cybersecurity expertise required to evaluate cyber defences across a wide spectrum of industries.

912,500 Man-hours of Expertise

K7's expert team is comprised of cybersecurity specialists who represent 912,500 man-hours of expertise in threat discovery, malware investigation, and attack remediation. K7's experts have the tools, skills, and perspective required to analyse enterprise IT as a cyberattacker would and quickly identify vulnerabilities that would be invisible to a technology-focused evaluation.

Superior Methodology & Processes

The methodology and processes followed by K7's team have been honed across numerous assessments of organisations operating in a wide variety of industries and jurisdictions, and are designed to be insightful, incisive, and actionable, enabling businesses to rapidly improve their cybersecurity posture and satisfy their compliance requirements.

K7 Labs

K7 Labs is one of the world's leading antimalware research and threat intelligence centres. The lab analyses hundreds of thousands of malware samples every day, has been the first discoverer of several malware, and is the first winner of the Real Time Threat List (RTTL) Contributor of the Year award from the Anti-Malware Testing Standards Organization (AMTSO). K7 Labs' state-of-the-art research facility enables in-depth investigation of, and the development of countermeasures against, any cyberthreat the modern enterprise might face.

Industry Partnerships & Leadership

K7's cybersecurity expertise is internationally recognised and has enabled K7 to form partnerships and collaborate with organisations that share our vision of cybersecuring the world.



Kesavardhanan J, the Founder of K7, also serves as the CEO of the Association of anti Virus Asia Researchers (AVAR) which fosters collaboration amongst international cybersecurity stakeholders.



The Global Cybersecurity Pioneer

India | Singapore | UAE | USA

www.k7cybersecurity.com