



K7 ISAP

Information Security Assurance Programme that
Establishes a State-of-the-art Cybersecurity Posture
in Digitally Enabled Organisations

www.k7cybersecurity.ae

Insufficient Protection Leads to Ineffective Enterprise Cybersecurity

Conventional enterprise cybersecurity initiatives usually involve an IT vendor installing cybersecurity products. Audits may be conducted occasionally based on regulatory and contractual compliance requirements. Internal IT teams monitor cybersecurity dashboards to note and resolve alerts.

Such measures are necessary, but not sufficient, to protect the enterprise in an environment of constant technology disruption and reinvention, expansion in the attack surface, and increased regulatory scrutiny. Digitally-enabled enterprises require integration of technology, internal and external mandates, and business processes to successfully mitigate cyber risk.

K7 Information Security Assurance Programme (K7 ISAP)

K7's Information Security Assurance Programme encompasses a framework of policies and procedures covering legal, physical, and technical controls involved in the information risk management processes of the modern enterprise. Services offered include discovering threats, assessing and improving security posture in real-time, prioritising weaknesses to address, and mitigating unseen vulnerabilities quickly and effectively by using specialised AI, automation, and gamification-based technology to achieve a state-of-the-art cybersecurity posture.

K7 ISAP – Benefits

- Secure Environment for Business Operations
- Relief from InfoSec Operational Concerns
- Periodic Reports
- Compliance Matrix with Intuitive Dashboard
- Contractually Defined SLAs and KPIs

K7 ISAP - Components

K7 ISAP enables our customers to be assured that the security features, practices, procedures, and architecture of an information system accurately mediate and enforce the organisation's security policy through various tools, techniques and practices, which include

- K7 External Security Posture Monitoring & Remediation Services
- K7 GRC Tools & Services
- K7 Vulnerability Management as a Service (K7 VMaaS)
- K7 Integrated Managed Services (K7 IMS)
- K7 Cybersecurity Training & Evaluation



K7 External Security Posture Monitoring & Remediation Services

Attack Surface Monitoring

Identifying and monitoring potential entry points into clients' networks.

Dark Web & Data Leakage

Scanning for sensitive information on the dark as well as surface web.

Brand Security

Protection against impersonation on social media, app stores, etc.

Analysis

Real-time Information Security Scoring and Risk Scenario Modelling.

Insight

Risk trend analysis for impactful reporting.

Remediation

Takedown services for malicious content.

K7 GRC Tools & Services

- An integrated approach to Governance, Risk, and Compliance, ensuring collaboration between risk, compliance, audit, cybersecurity, and sustainability teams
- Identify, assess, manage, and mitigate strategic risks, data-centric risks, operational and enterprise risks, IT and cyber risks, third-party risks, fourth-party risks, compliance risks, and environmental, social engineering, application, infrastructure, and governance risks

K7 Vulnerability Management as a Service (K7 VMaaS)

- Helps clients identify and prioritise threats
- Implements vulnerability exposure response on behalf of the organisation
- Agile process offering continuous enterprise IT ecosystem monitoring with Asset Discovery, Prioritisation, Vulnerability Assessment, Reporting, Remediation, Evaluation and Verification
- A vulnerability management system that immediately flags the most critical vulnerabilities. Contextual input, such as business, exploitation, threat, and risk data are assimilated and mitigation recommendations for identified vulnerabilities are generated

A man in a dark suit is standing and presenting to a group of people seated at desks in a modern office. Large windows in the background show a cityscape. The scene is dimly lit, with light coming from the windows and a computer monitor on the left.

K7 Integrated Managed Services (K7 IMS)

- Minimises time required to respond to an alert, remediate the problem, and successfully manage the incident
- Consolidates cyber risks into a single reportable model
- Real-time and continuous visibility into security concerns
- Scorecards to gauge risk remediation performance on a continual basis
- Integration of people, processes, and technology (SIEM, SOAR, ETI, MDR, ML, IDS, NBAD, VAPT, UEBA, Regulatory compliance)

K7 Cybersecurity Training & Evaluation

- Cybersecurity awareness and cyber hygiene training, including discussions on cyber law and social media hazards, customised to suit the functional responsibilities of different teams
- Case-study-based analysis of cyberattacks
- Tests to evaluate knowledge gained
- Simulated attacks to evaluate trainee response and gauge the effectiveness of training

Why K7?

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.

Superior Methodology & Processes

The methodology and processes followed by K7's team have been honed across numerous cybersecurity assignments in 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.

912,500 Manhours of Expertise

K7's expert team is comprised of cybersecurity specialists who represent 912,500 manhours 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 software-only evaluation.

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.



India | Singapore | UAE | USA

businessenquiry@k7computing.com

www.k7cybersecurity.ae



K7 Cyber Security FZCO,
IFZA Business park, Building A1,
Dubai Silicon Oasis, Dubai, UAE



businessenquiry@k7computing.com



+ 971 56 367 2864

June 2023