2024

Information Security, Privacy, and Computer Forensics

Tenet Services

tenet

Tenet services

In the modern world, information is one of the most valuable assets for an organisation, and information and communication technologies underpin nearly all business processes. The idea that “whoever controls information controls the world” has never been more relevant. Information has a huge impact on many processes in society, and properly structured data protection is a key condition for ensuring a company’s competitiveness and sustainable development.

We believe that the effectiveness of an information security system is primarily achieved through its comprehensiveness: the system should cover both organisational/ methodological and technical issues.

Tenet offers a wide range of services that cater to all aspects of information protection.

01

Penetration Testing and Social Engineering

We make a practical assessment to ascertain the possibility of unauthorised access to a company’s critical data from the Internet, as well as from its internal network. During the testing process we search for potential compromise routes based on any vulnerabilities identified, or a combination of such vulnerabilities. We also assess potential breaches using human-factor-based attacks and techniques. For example, a phishing attack is carried out by sending mass emails that appear to be from internal departments or known contacts. Any email recipient who opens the message, clicks on links within it, opens attachments, or enters their username and password on a fake website will be tracked.

02

Analysing the security of network infrastructure and application systems

The network infrastructure – firewalls, wireless networks, routers, switches, VPNs, etc. – forms the backbone of any information system. As part of this service, we examine an organisation’s network infrastructure configuration and related processes from an information security perspective, and assess their efficacy based on leading global practices and information security standards. The analysis of the security of application systems, as well as mobile and web applications, comprises both automated and manual procedures to detect weaknesses. Appropriate methodologies and approaches are used for each application (including the OWASP Testing Guide, OSSTMM, WASC Threat Classification, STRIDE) to cover as many potential attack vectors as possible.

03

Information security Incident Response and Investigation

Information security incidents can cause significant damage to modern organisations, and may involve not only compromising information systems but also bypassing processes and deceiving people. We assist clients in responding to information security incidents, determining their nature and circumstances, mitigating the impact, and reducing damage. The incident response stage transitions smoothly to an investigation phase, after which we provide detailed advice and guidance on the measures that need to be taken to prevent such incidents from reoccurring. The main goal is to help a company contain the spread of the incident and subsequently restore its business operations. In addition, we help collate incident data in such a way that it can be used as legally significant evidence in court.

04

Computer forensics

Using specialised equipment and state-of-the-art high-tech software we assist clients in the process of collecting necessary electronic information and ensuring the preservation of evidence during its transfer and processing. We perform a range of forensic computer examinations, including:

- the recovery and analysis of deleted data
- ascertaining any incidents of deliberate data deletion
- reconstructing the incident timeline
- analysis of user activity, internet history, instant messaging, installed software, and more

05

Development of Strategy, Process Improvement, and Information Security Risk Analysis

We conduct an analysis of information security functions and processes, in accordance with a number of related international standards (for example, ISO/IEC 27001-2:2022, CIS Critical Security Controls V8, NIST Cybersecurity Framework, and ISF Standard of Good Practice for Information Security 2022). Based on the analysis results, we elaborate recommendations related to setting up, implementing, and improving information security processes in a company (for various planning horizons), and then formulate a long-term information security development strategy, taking into account the organisation’s particular business strategy. We also perform an information security risk analysis using the FAIR and ISF QRA methodologies, the results of which help to not only determine the current state of the company, but also to plan and prioritise initiatives to develop the information security function.

06

Services related to processing and safeguarding personal data

We take stock of processes related to processing and safeguarding personal data, and identify applicable privacy legislation in any country in the world: the European Economic Area (GDPR), China (PIPL), Turkey (PDPL), Singapore (PDPA), Egypt (PPD), UAE, Serbia, CIS countries, etc. We draw up a list of specific actions to be taken to eliminate any identified inconsistencies with applicable legislation, elaborate (update) the drafts of required documents, coordinate the initiation of privacy management processes, assist in analysing privacy risks, train employees and contractors, and provide consulting support if regulatory bodies seek information or request a scheduled or unscheduled inspection. We are also ready to advise on other non-standard issues in the field of personal data.

07

Intelligent data analysis (eDiscovery)

Often, as part of legal cases, at the request of regulatory bodies or during an internal investigation, companies need to search for emails and documents in a large volume of available information. We assist with copying, processing, and reading digital data, including electronic correspondence, regardless of the volume of information involved, and we also analyse selected data by keywords. In addition, we help record electronic data that can be admissible in court as electronic evidence. Visual analysis tools and machine learning technologies can significantly reduce the time it takes to get to the really pertinent data. eDiscovery solutions are also used effectively to identify fraudulent schemes, search for withdrawn assets, and analyse the actions of intruders.

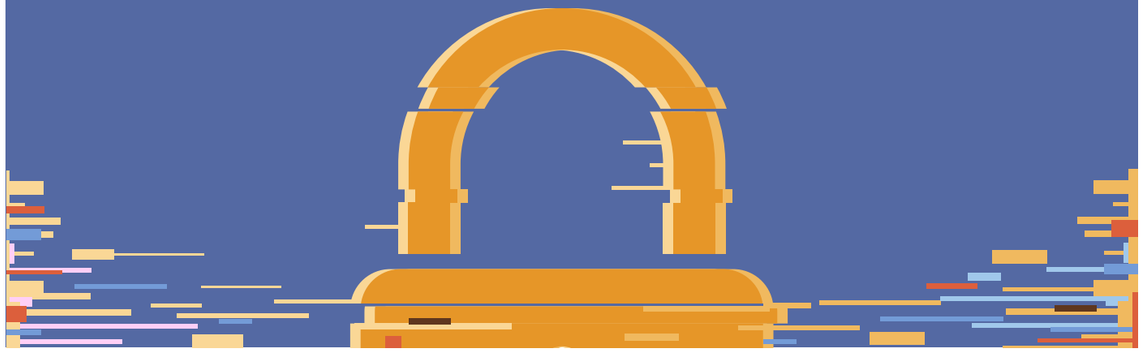
Why Tenet

Our team is made up of world-class professionals who hold such certificates as CISA, CISM, CISSP, C|EH, OSCP, CRISC, and ISO 27001 LA (a).

We have no conflicts of interest stemming from affiliations with vendors, service providers, or developers.

The results of our work are clear and comprehensible, not only to technical specialists, but also to a company’s management.

We take a comprehensive and integrated approach to resolving information security issues, and pay attention to both organisational and technical aspects.



Contacts

Marina Makarova
Senior Consultant

+381 61 2823 347
marinamakarova@tenetoffice.com

www.tenetcons.com