Deloitte.

Red teaming

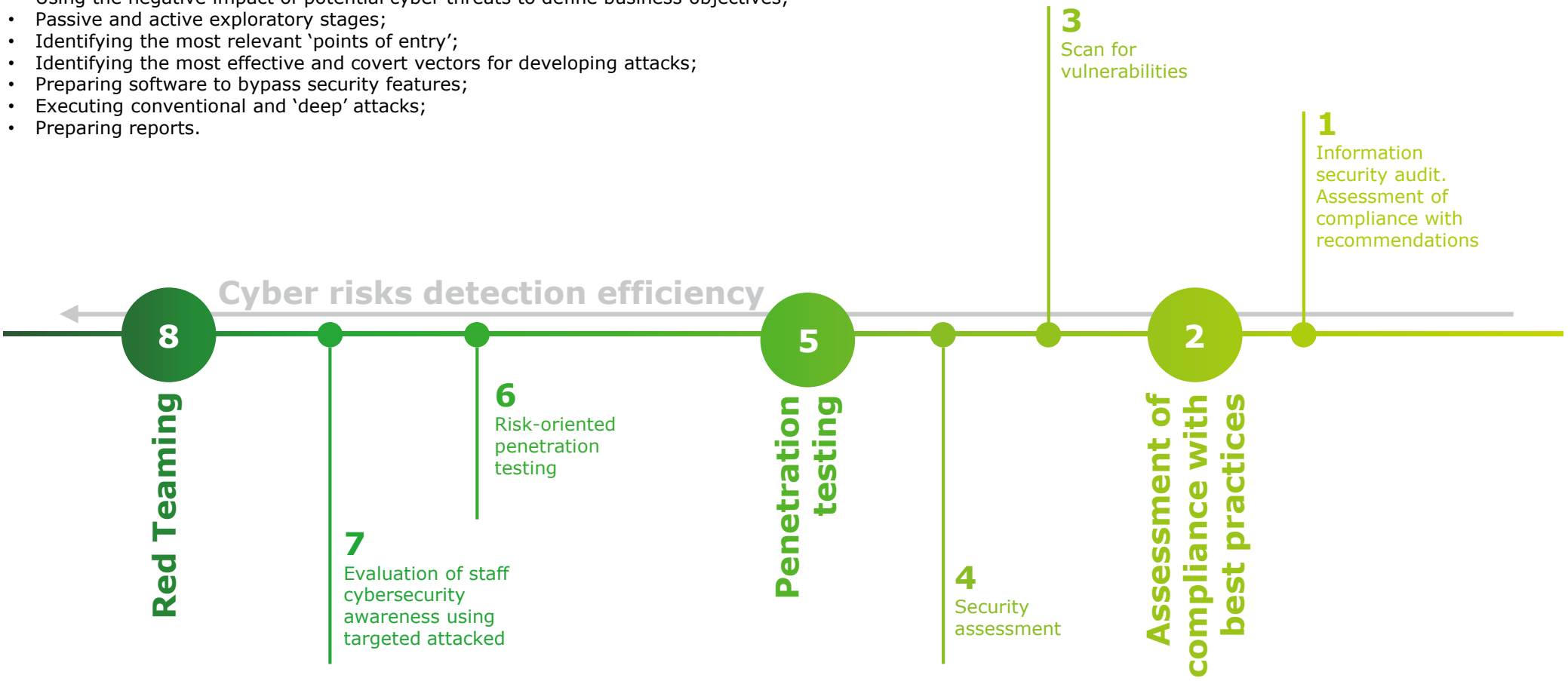
Cyber threat modelling

The exponential growth of technology and ever-expanding use of computers has led to the emergence of new types of risk, which the use of traditional security testing methods cannot prevent. The number of cyber incidents is rising every year along with the damage inflicted by these attacks. For this reason, organizations must prepare themselves for the limitless dangers posed by real attacks. Information system security assessments, evaluations of staff cybersecurity awareness and penetration testing are all useful solutions, but are not flexible enough to fully protect against the real attack surface.

Red teaming is flexible, target-orientated and is not confined to the limitations of testing. It does not use standard templates and assesses the response readiness to incidents by allowing the exploitation of critical vectors. Red teaming means attempting all possible methods to accomplish any objective an attacker may have: physical access, social engineering attacks, covert penetration, etc.

Our red teaming approach involves:

- Using the negative impact of potential cyber threats to define business objectives;
- Passive and active exploratory stages;
- Identifying the most relevant 'points of entry';
- Identifying the most effective and covert vectors for developing attacks;
- Preparing software to bypass security features;
- Executing conventional and 'deep' attacks;
- Preparing reports.



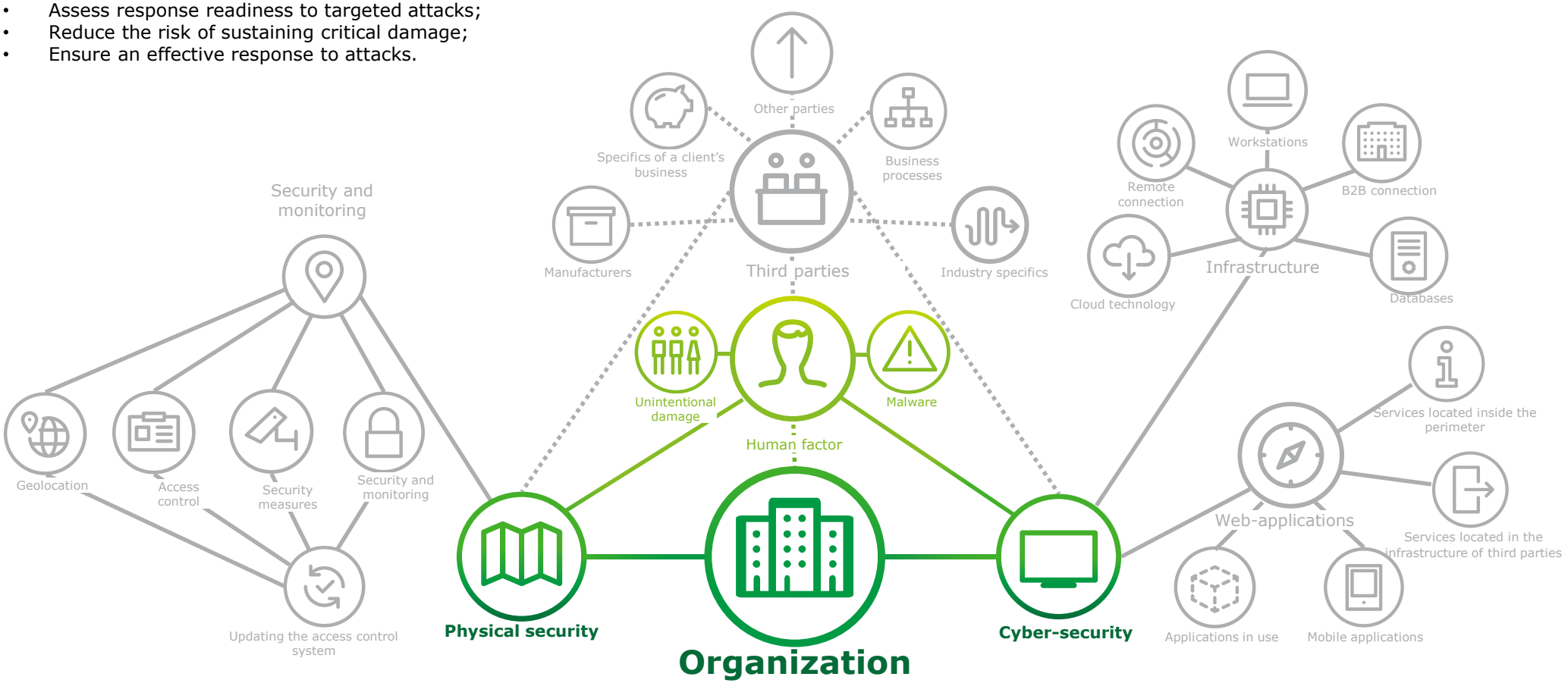
The attack surface

Assessing the detection and response capabilities of an organization is a complex and unconventional process. The use of standard techniques during testing could significantly affect the results and reduce their reliability. We do not use any templates during a red team event; our methodology is aimed at objectively demonstrating an organization's capabilities to resist complex, new and targeted attacks. The goal of testing is not to check all possible vectors, but to identify the critical exposed areas, find the most effective and covert vectors, conduct targeted controlled attacks, and then record and analyze the results to increase the overall level of resistance to threats.

The sheer number of parties that interact with an organization generates an enormous number of connections, each one entailing specific threats and creating potential attack vectors. The report will include data on the testing results for physical security and cyber-security, as well as human factors and information about the current threats facing an organization. An analytical breakdown will give a risk assessment, an evaluation of incident detection and cyber threat resistance, as well as a list of recommendations for strengthening the information security system and boosting resistance to targeted attacks.

Our approach enables us to:

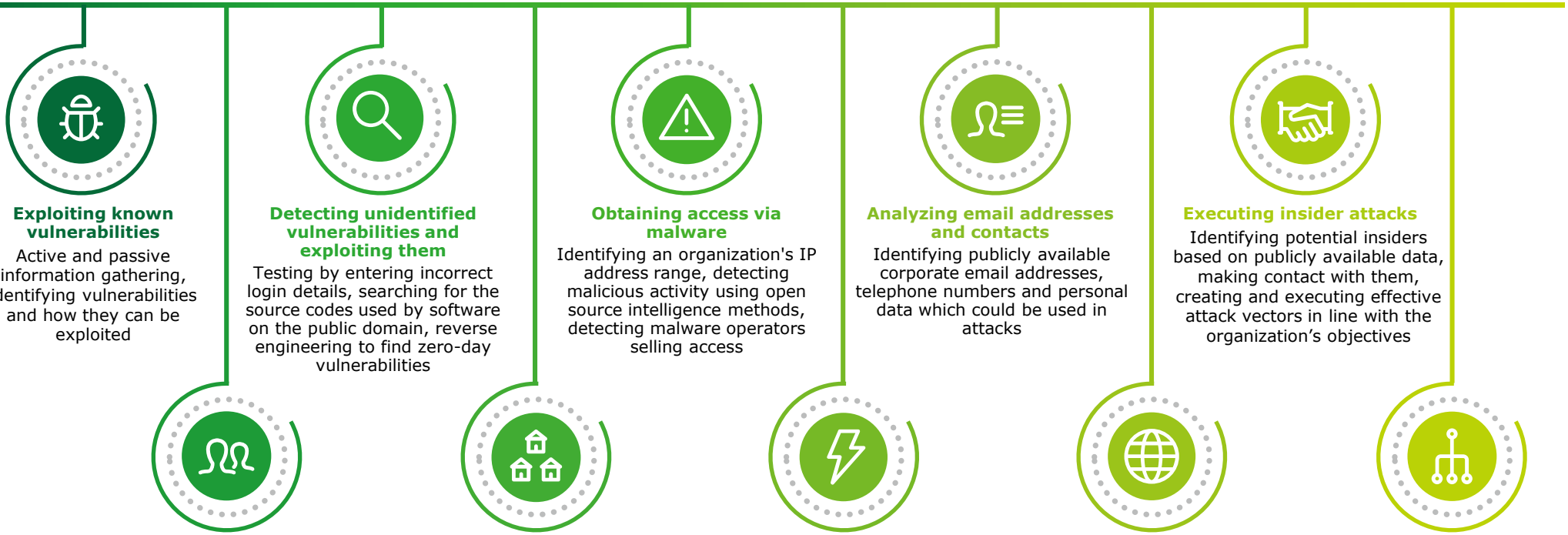
- Assess response readiness to targeted attacks;
- Reduce the risk of sustaining critical damage;
- Ensure an effective response to attacks.



Methods used in attack modelling

Testing that is tailored specifically to an organization involves determining and executing attack vectors, taking into account industry-specific processes, publicly available information about key assets, the business environment, the IT and physical infrastructure, as well as the overall maturity level of cyber-security functions.

Our approach involves the use of non-destructive testing methods. If there are business continuity risks, we coordinate the next steps with key decision-makers at the client organization.



Exploiting known vulnerabilities

Active and passive information gathering, identifying vulnerabilities and how they can be exploited

Detecting unidentified vulnerabilities and exploiting them

Testing by entering incorrect login details, searching for the source codes used by software on the public domain, reverse engineering to find zero-day vulnerabilities

Obtaining access via malware

Identifying an organization's IP address range, detecting malicious activity using open source intelligence methods, detecting malware operators selling access

Analyzing email addresses and contacts

Identifying publicly available corporate email addresses, telephone numbers and personal data which could be used in attacks

Executing insider attacks

Identifying potential insiders based on publicly available data, making contact with them, creating and executing effective attack vectors in line with the organization’s objectives

Social engineering attacks

Active and passive information gathering, detection and implementing the most effective attack vectors

Obtaining physical access

Testing access controls, physical security measures and monitoring systems

Executing network attacks

Conducting man-in-the-middle attacks (aimed at intercepting data), as well as exploiting network misconfigurations.

Attacks using publicly available data

Gathering data from social media, analyzing metadata, detecting leaks and indexable critical elements for the future creation and exploitation of vectors

Executing combined attacks

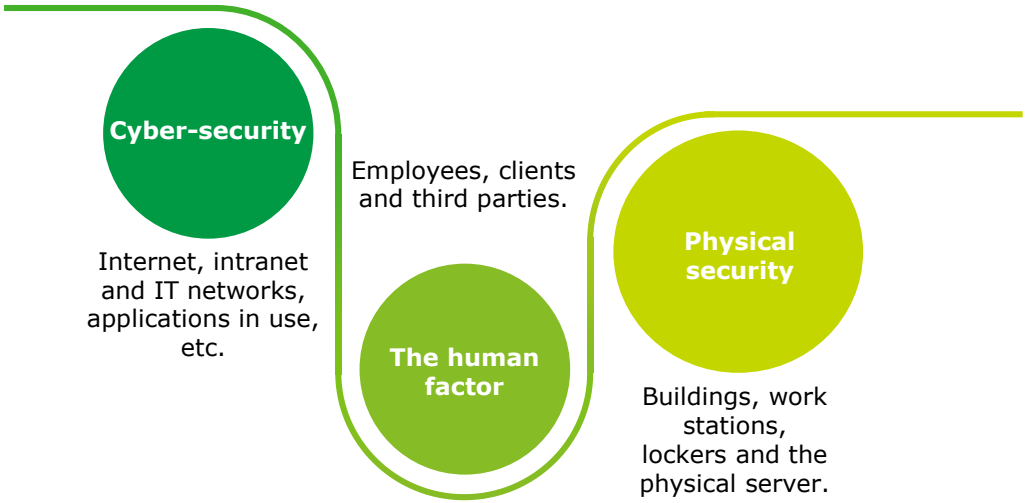
While drawing up lists of vectors, we combine and adjust the methods used to ensure they are in line with the organization's objectives

The realistic approach

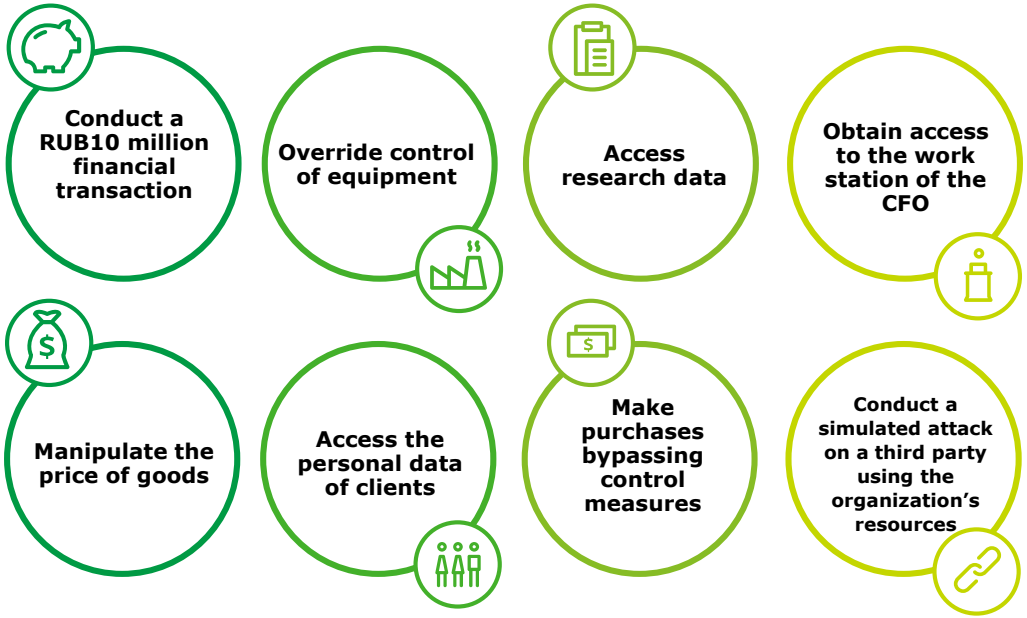
The risks of complex attacks cannot always be detected by routine security assessments. Controlled attack scenarios that cover a variety of security aspects, based on well-established methodologies and focused on achieving concrete goals, objective assess a security team's performance. To ensure maximum realism, our specialists are constantly analyzing the objectives, methods, techniques and tools employed by various hacker groups when selecting possible attack vectors and its implementation.

Cybersecurity should not be seen in isolation from checkpointing, which is embedded into business processes to ensure reliability. The human factors means that it is essential to build a multi-layered security system for an organization's assets. Our approach gives an objective assessment of the reliability of the business environment, reducing the risk of social engineering attacks by creating an effective and well-functioning control system for each business process.

Key principles



Threat model



Our skills

Our team of specialists, which includes the winners of the 2018 PHDays ethical hacking competition and the 2017 Cyberlympics meet, have extensive experience in conducting penetration testing, assessing how configurations correspond to best practices and developing recommendations, as well as assessing and auditing information security.

Our specialists' skills are backed up with internationally recognized qualifications (CISSP, CISM, JSO27001, COBIT, JTIL, CDPP, CEN).

Gartner has selected Deloitte as the leader in Security Consulting for the sixth year running (source: Gartner, Market Share Analysis: Security Consulting Services, Worldwide, 2017, Elizabeth Kim, 27 June 2018.).

ALM Intelligence, formerly Kennedy, said that Deloitte develops, tests and uses cutting-edge methodologies, reflecting a deep understanding of their clients' information security systems and helping companies build world-class protection against cyber threats (source: ALM Intelligence; Cybersecurity Consulting 2017; ALM Intelligence estimates © 2017 ALM Media Properties, LLC. Reproduced under license.).

Contacts

Denis Lipov
Partner
Risk Advisory
dlipov@deloitte.ru
+7(495)787-06-00 (ext. 3071)

Ivan Nagornov
Assistant Manager
Risk Advisory
inagornov@deloitte.ru
+7(495)787-06-00 (ext. 8281)

Deloitte.

deloitte.ru

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 264,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.