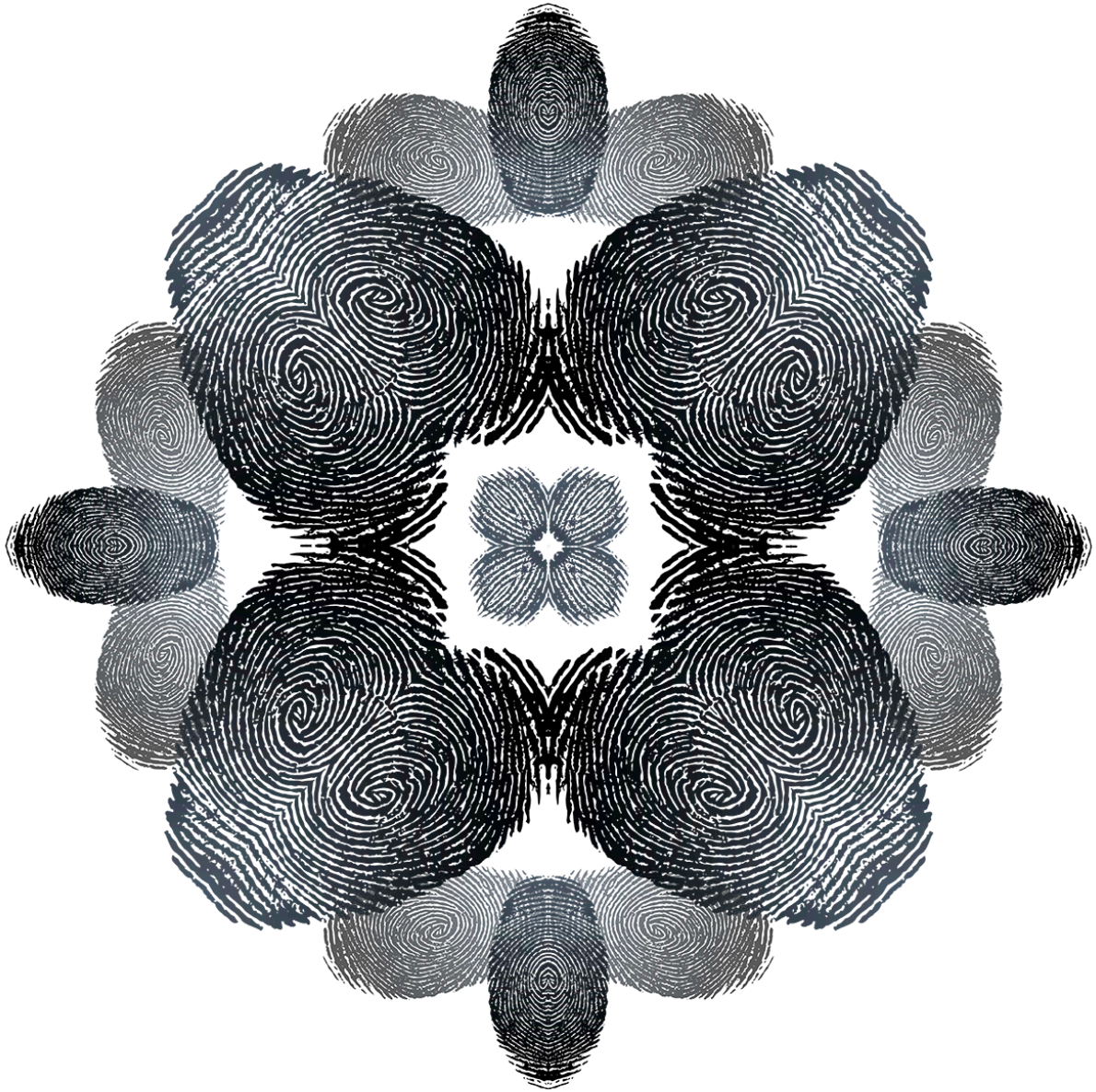
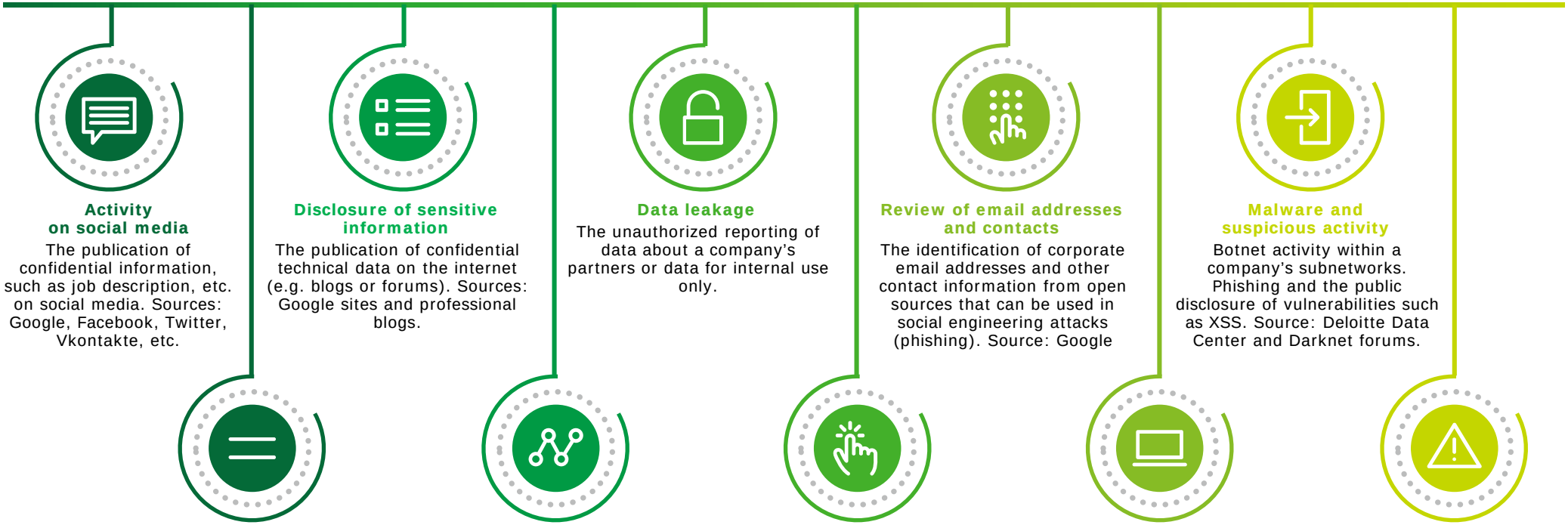
Deloitte.



Cyber Threat Footprint

Cyber Threat Analytics

The deliverable of the service is a cyber security status report and an analysis of the tolerance of a company's business processes to attacks from the use of information available from open sources. The assessment is conducted in accordance with the OSINT methodology, covering the key areas specified below:



Activity on social media

The publication of confidential information, such as job description, etc. on social media. Sources: Google, Facebook, Twitter, Vkontakte, etc.

Disclosure of sensitive information

The publication of confidential technical data on the internet (e.g. blogs or forums). Sources: Google sites and professional blogs.

Data leakage

The unauthorized reporting of data about a company's partners or data for internal use only.

Review of email addresses and contacts

The identification of corporate email addresses and other contact information from open sources that can be used in social engineering attacks (phishing). Source: Google

Malware and suspicious activity

Botnet activity within a company's subnetworks. Phishing and the public disclosure of vulnerabilities such as XSS. Source: Deloitte Data Center and Darknet forums.

Host data

The collection of information about hosts (servers, desktops, databases) and the versions of apps in use, thereby listing vulnerabilities and public exploits for them. Source: Google, LinkedIn, Vulnerability Databases, Net Craft, Network Utilities, and Robtex.

Network data

Detailed information about network addresses, network devices and related vulnerabilities available in cyberspace. The analysis of requests for corporate resources. Source: Google, LinkedIn, Vulnerability Database, Net Craft, and Network tools.

Data about domains and DNS names

The passive identification and listing of domains and DNS names. Source: Net Craft, Network Tools, and Robtex.

Metadata analysis

The collection and evaluation of webpage content and the a company's corporate resource files that can be used to develop internal attacks. Source: www.metaheaders.com and Google.

Technical misconfigurations

The identification of known configuration vulnerabilities on websites and other publicly accessible servers that can be used by attackers to gain unauthorized access. Source: company websites, specialized search engines, vulnerability disclosure sites.

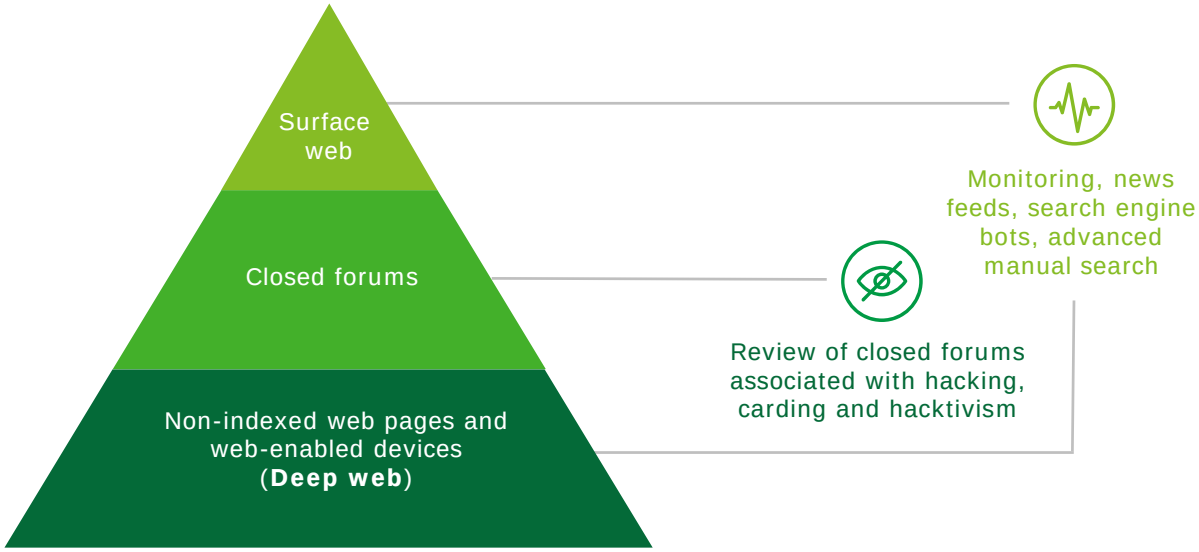
Scope of Analysis

The Deloitte Global Center for the collection and analysis of cyber threats provides services on a 24/7 basis and analyzes the data obtained through searching, extracting, filtering, and monitoring.

Cyber Threat Analytics forms the basis of the open source-based risk assessment. This is carried out for external events that arise from outside the company.

Deloitte analysts process massive amounts of data from public sources and closed forums.

We monitor the surface web and non-indexed web pages using automatic tools. We use advanced manual search if monitoring processes cannot be automated.



We allocate significant resources to manually verify and investigate potential cyber threats against our clients as this is the key element in ensuring the reliability and value of data obtained. Our analysts are specialists in data retrieval and processing, conducting research to continually improve our cyber threat detection solutions.

Key Sections of the Cyber Threat Footprint Report 1/2

The report will give information regarding the actual threats facing an organization, a risk assessment, and the key findings and recommendations to mitigate the risks from the threats identified.

Area	Overview
Cybersquatting	• We identify cases where domain names containing a trademark owned by another party have been registered with the intention of either reselling them or using them for illegal activities. • We identify activity sources for these domains.
Phishing	• We identify social engineering activity aiming to obtain sensitive information, such as usernames, passwords, bank details, or to access to the corporate network.
Malware	• We identify malware developed to damage hardware or infiltrate the corporate environment by using signatures and analyzing program behavior in the secure environment; • We provide continuous monitoring of botnets and assistance in deleting stolen data.
Sensitive information leaks	• We identify leaks of confidential information and access to such information by unauthorized users based on the Ad Hoc search functionality; • We perform an analysis of the information available on open source databases to identify sensitive information relating to the organization, such as signatures, password hashes, corporate accounts, email addresses, mutual settlements with partners, documents for internal use, etc.
Cyber-attacks	• We collect evidence of cyber attacks targeting the company's IT assets and processed data. Sites are analyzed and considered when investigating new attacks.

Key Sections of the Cyber Threat Footprint Report 2/2

Area	Overview
Cyber-attack vectors	• We identify ways threats can be implemented and infiltrate the corporate network; • We identify traces of infection on the company's IT assets; • We perform real-time analysis of changes in the web-accessible IT environment and identify weaknesses in the reconfigured IT landscape.
Hacktivism	• We identify traces of the use of workstations, the corporate and computer networks to initiate actions on the web; • We assess the need to launch information campaigns to increase staff awareness and prepare employees for potential social engineering attacks; • We identify the threat hacktivists pose to the organization and, based on this, prepare for future phishing attacks, DDOS attacks, etc.
Mobile apps	• We analyze apps available for download from unofficial sources (Git repositories, cloud storage, etc.) for malware. The apps can exploit and hide behind the high level of trust and confidence in the company's brand, posing a high risk of compromising user devices as well as the risk of reputational damage to the company.
Fraud in social media	• We identify unauthorized profiles in social media using the same name as the company, as well as comments to legitimate profiles connected to fraudulent activities.
Other frauds	• We identify suspicious activities indicating fraud that cannot be included in any of the above categories. These may include, for example, scams, clickfraud, etc.

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.