DCSO Whitepaper

Internet Exposure Monitoring (IEM)

Internet Exposure Monitoring (IEM) as a Managed Service

Regain control over your digital visibility and threat exposure

Trade secrets, personally identifiable information, or your marketing strategy freely accessible to everyone on the Internet? At the latest when you share information within your supply chain or with service providers, you lose control over what happens with your data. Due to lack of due diligence in data handling, infrastructure misconfigurations, negligence, or simple human errors sensitive or often confidential information is regularly exposed in publicly available storage protocols, cloud services, or freely accessible databases. As a result, this data might be found and misused by anyone. The associated risk for the entire company is high, especially as most of the leaks of this kind are never noticed internally.

Identities are an valuable asset for the criminals. Therefore malicious actors regularly breach into websites and databases to steal the data. The stolen credentials and further personally identifiable information (PII) enable the criminals to conduct different types of attacks, from a phishing email, through an account takeover to a more sophisticated CEO fraud campaign, the criminal' attack portfolio is large. Through credential stuffing, attackers are able to test stolen credentials on other platforms, e.g. your company network, and can thus penetrate your company's networks. It takes several months or even years before a data breach becomes public. Before that, the access data has already been misused and resold several times.

DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
EUREF Campus 22, 10829 Berlin, Germany

What is IEM?

To keep these threats in focus DCSO GmbH has established a Managed Security Service - Internet Exposure Monitoring (IEM). IEM detects, analyzes, and reports leaked sensitive company information, exposed online through either negligence along the supply chain or insiders, or which is available on Dark Web forums due to active exfiltration by external attackers. Thanks to the service, the spread of internal company information can be stopped and appropriate remediation measures can be taken. Furthermore, customers gain better visibility and understanding of threats that are beyond their control and can better protect both their employees and the company from attacks.
To cope with the risks, we developed two complementary solutions.

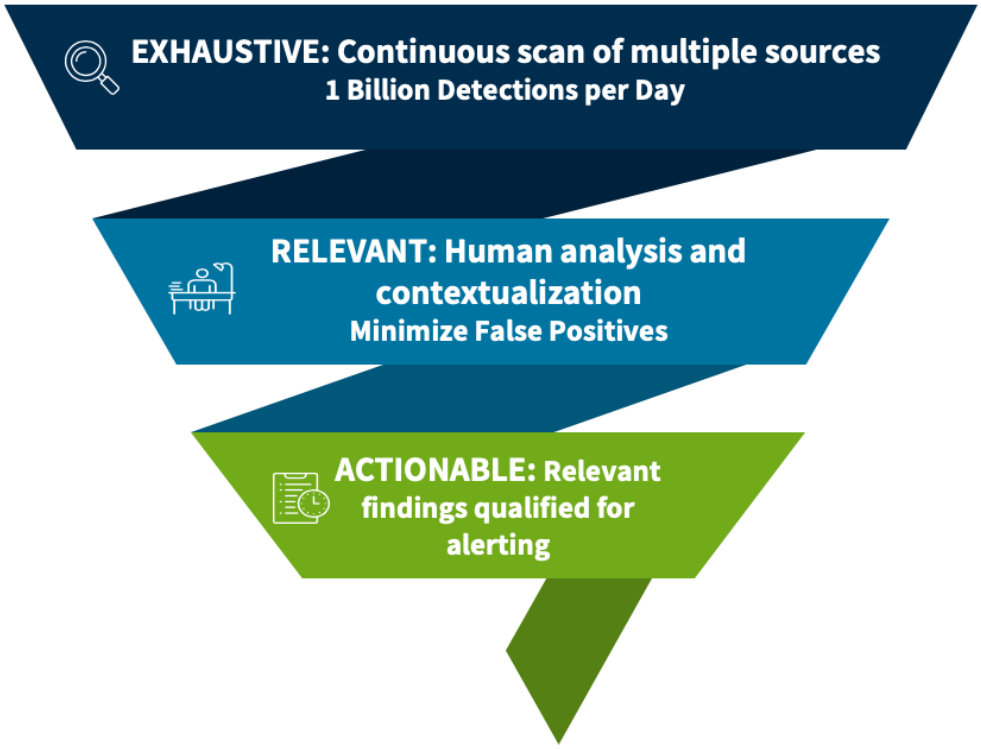
1. Information Leakage Monitoring Service (ILM)

In order to detect leaked sensitive information, the ILM service continuously scans all layers of the internet and analyzes and evaluates the information that is freely available.

The scan covers the following areas:

- over 100 million websites incl. Dark Web forums
- the complete publicly routable unicast IPv4 space
- cloud services and much more

Furthermore, our experts identify the leaked information concerning your company and inform you immediately about potential security findings in the form of a comprehensive and actionable report. This report not only includes an assessment of the potential risks based on the content of the leaked information or its origin and attribution, but it also adds relevant context including all necessary information for efficient remediation measures.



Information Leakage Monitoring proactively enables customers to stay ahead of the curve and to identify suppliers, business units, and regions with high leak rates. These high-risk areas can then be subjected to extensive monitoring, increased awareness training, or further organizational and technical measures.

Many companies learn about previously unknown data leaks for the first time through us. Make sure that sensitive documents, personal data, and your intellectual property do not fall into unauthorized hands. With the Information Leakage Monitoring (ILM) of DCSO GmbH you keep control of your digital footprint!

2. Identity Leakage Monitoring (IDLM)

If attackers have breached a database, the stolen credentials are usually sold in Dark Web forums. This is where our Identity Leakage Monitoring (IDLM) comes in. Our primary goal is to provide information to our customers about their stolen identities as quickly as possible. This is achieved by the unique intelligence collection using technology and HUMINT (an exclusive network of private sources and partners). In this way, we learn about a new data breach as soon after the initial breach as possible.

As soon as we identified relevant information regarding our customers in the data breach we inform the concerned company immediately.

Our analysts create customized reports that help to increase the effectiveness of remediation measures through classification and customer-specific categorization such as VIP prioritization and data freshness assessment. In addition to the prepared data, statistical analyses, risk assessments, and recommendations for appropriate remediation measures are provided. Our scoring mechanism to depict metrics over time and comparison within customers' peer groups enable customers to understand their own exposure and focus on high-risk areas.

Prevent unauthorized access to your systems before it is too late.

Quicksearch and PoC

To see how our service works, we offer you the opportunity to test it in detail.
First of all, we will show you how it works in a Quicksearch presentation, as well as possible results from continuous monitoring. Afterwards, you will have the opportunity to convince yourself within a PoC.

About the author

DCSO is a Berlin-based cyber-security joint venture, founded in 2015 by Allianz, Bayer, BASF, and Volkswagen. We provide security services and enable synergies between our customers.

Visit us on https://dcso.de/services/internet-exposure-monitoring/
Get in touch: sales@dcso.de