Socura

Dark Web Monitoring (DWM) Service Definition

hello@socura.co.uk

Table of Contents

Service Description

Dark web monitoring is the practice of monitoring the dark web, which is a part of the internet that isn't indexed by traditional search engines and is often associated with illegal activities. The dark web is known for hosting marketplaces for illegal goods, illicit activities, and other clandestine operations.

Dark web monitoring involves using specialized tools and techniques to track and analyze the dark web for mentions of specific information, such as stolen data, personal information, or intellectual property. Organizations, cybersecurity firms, and individuals use dark web monitoring to proactively detect if their sensitive information has been compromised or is being traded on the dark web. By monitoring the dark web, they can take steps to mitigate potential damage, such as informing affected parties, enhancing security measures, and working with law enforcement.

Dark web monitoring is valuable for several reasons, especially in today's digital landscape where cybersecurity threats are prevalent. Here are some reasons why Socura recommends organizations might consider implementing dark web monitoring:

- **Data breach detection:** Dark web monitoring can help organizations detect if their sensitive data, such as customer information, login credentials, or financial details, has been compromised and is being traded or sold on the dark web. This early detection can allow them to take swift action to minimize the impact of a data breach.
- **Proactive security measures:** By monitoring the dark web, organizations can proactively identify potential threats and vulnerabilities before they are exploited by threat actors. This can help in strengthening their security posture and implementing additional protective measures.

- **Intellectual property protection:** Companies can use dark web monitoring to identify if their intellectual property, such as proprietary software, designs, or trade secrets, is being illicitly shared or sold on the dark web.
- **Fraud prevention:** Individuals can use dark web monitoring to detect if their personal information, such as social security numbers, credit card details, or login credentials, has been compromised and is being misused for fraud or identity theft.
- **Regulatory compliance:** In certain industries, regulatory standards require organizations to monitor for potential data breaches and unauthorized disclosures of sensitive information. Dark web monitoring can help in meeting these compliance requirements.

Socura's Dark Web Monitoring & Response Service

Dark web monitoring provides a proactive approach to cybersecurity, allowing organizations and individuals to stay ahead of potential threats, protect sensitive information, and mitigate the impact of data breaches.

Socura's Dark web monitoring and response service offers several benefits for organizations concerned about their cybersecurity and the protection of sensitive information. Some of the key benefits of dark web monitoring include:

- **Early Detection of Data Breaches:** Dark web monitoring can provide early detection of data breaches, allowing organizations to take immediate action to mitigate the impact and protect affected individuals.
- **Proactive Threat Intelligence:** By monitoring the dark web, organizations can gain insights into potential threats and vulnerabilities, enabling them to proactively enhance their security measures and preemptively address emerging risks.

- **Protection of Sensitive Information:** Dark web monitoring helps in safeguarding sensitive information, such as personal data, financial details, and intellectual property, by identifying instances of unauthorized exposure on the dark web.
- **Compliance with Regulations:** For organizations operating in regulated industries, dark web monitoring can support compliance with data protection and privacy regulations by demonstrating proactive efforts to monitor for potential data breaches and unauthorized disclosures.
- **Fraud Prevention:** Individuals can use dark web monitoring to detect if their personal information has been compromised, helping them take steps to prevent identity theft and fraud.
- **Reputation Management:** Timely detection and response to data breaches or unauthorized disclosures on the dark web can help organizations protect their reputation and maintain trust with customers and partners.
- **Enhanced Security Posture:** By incorporating dark web monitoring into their cybersecurity strategy, organizations can strengthen their overall security posture and reduce the likelihood of successful cyber attacks.
- **Incident Response Readiness:** Dark web monitoring provides valuable information that can inform incident response plans and help organizations respond effectively to security incidents.
- **Brand Awareness:** Through awareness of how your brand is being represented or misused on the dark web, Socura's clients can take early action to mitigate risks, protect their reputation, and secure their intellectual property and customer data.

Service Operations

The Socura Customer Success service is focused on delivering exceptional value into our customers. The Customer Success Manager collaborates with each customer to agree key Customer Success goals. Key activities include:

- Managing and maintaining the service in line with the contracted service levels
- Securing the required resources, where applicable, to ensure successful service delivery against the overall service aims
- Management of service escalations and communications
- Identifying and managing any risks associated with the service delivery
- Holding monthly review meetings with customer stakeholders to the agreed schedule
- Monitoring and managing the progress of the partnership against the agreed customer success strategy and service activities
- Maintain and increase solution and services adoption
- Maximise customer satisfaction and experience
- Implement customer success service improvement initiatives
- Identify any adoption barriers and work with customers to remove them
- Identify emerging technology and innovation opportunities
- Management of renewals for both value-added services, maintenance and well as subscription services
- Securing all resources required to successfully deliver the customer success strategy

Service Transition

The Transition Manager has overall control of onboarding activities and is:

- Responsible for monitoring and managing the progress of the onboarding activities against the agreed plan and activities
- Responsible for monitoring and managing changes to the transition plan to minimise impact
- Securing all resources required to successfully deliver the transition
- Ensuring the aims of the transition continue to be aligned with evolving business needs
- Recommending future action on the transition where tolerances are exceeded

Ordering and Invoice Processes

Orders can be placed by completing the G-Cloud ordering process. We encourage customers to contact us using the details contained within our G-Cloud page to allow us to support you with any queries.

Invoicing will take place annually in advance based on the agreed contract that has been put in place between the customer and Socura Ltd. Invoices are payable within 30 days.

Information Security

Socura is committed to ensuring the highest standards of data quality, data protection, integrity, confidentiality, and records management are met in compliance with the relevant legislation.

Socura holds security-based accreditations, including ISO 27001, Cyber Essentials Plus, and has certified against the Data Security and Protection toolkit to the Standards Exceeded rating, which evidences Socura's commitment to information security management.

All staff involved with the development, implementation, and operation of the Socura MDR service are background checked to the BS7858 Security standard, and are trained and aware of the security policy commitments to be undertaken to ensure compliance:

- Confidentiality: ensuring only authorised persons have access to information.
- Integrity: ensuring validity, accuracy, and completeness of information.
- Availability: ensuring information, associated assets, and systems can be accessed when required by authorised persons.
- Regulatory Adherence: adheres to regulations, laws and codes of practice in each country where it operates.
- Assurance that Socura management and employees comply with the Socura Security Policy in the management of information, hardware, firmware and software.
- Minimised risk of damage to assets, information, reputation, hardware, software or data.
- Follow a systematic approach to risk assessment and treatment.
- Work towards continuous improvement

Pricing

Pricing is per the pricing sheet available on the Socura G-Cloud page.

Further Information

If further information, or clarification is required, please contact hello@socura.co.uk