CYNODE.

Dark Web and Brand Monitoring

Data sheet

Cynode's Dark Web & Brand Monitoring Service

Cynode's Dark Web & Brand Monitoring service is one of the most comprehensive cyber intelligence services available on the market. It combines dark web monitoring and brand monitoring, addressing a wide range of use cases.

Using Cynode Ultima Platform's monitoring tools and through research, Cynode cyber analysts identify indicators of possible breaches, data leaks, attack preparations, and other malicious activities, validate these findings, and initiate appropriate response processes.

Defining Dark Web & Brand Monitoring

Dark Web Monitoring: Dangers and Opportunities Go Hand in Hand

Cyber attacks do not happen from one second to the next. Threat actors go through a diligent preparation phase before launching their attacks. This phase may take days, weeks, months, or even years, during which threat actors look for weaknesses in their targets' attack surface, may communicate with each other, and build their tools. The anonymity that the dark web provides offers a good hiding place for threat actors.

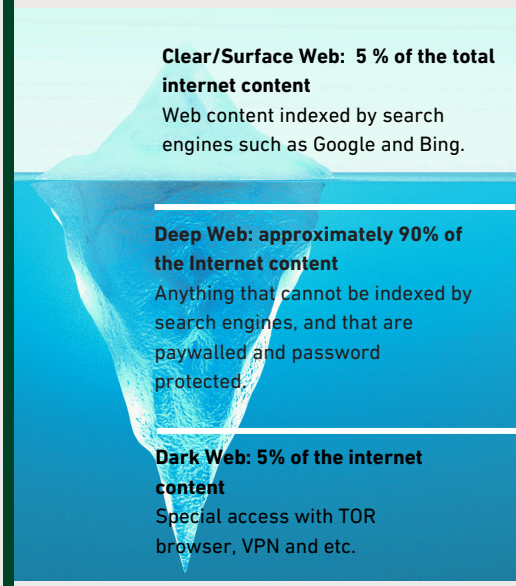
This phase also means a window of opportunity for cyber defense teams. If any indicators of such preparations can be identified, cyber threats can be tackled early on, saving time, money, and eliminating risk.

Brand Monitoring: A comprehensive surveillance of companies' digital footprint

Any company-related information and properties gathered in one attack can be used in another. The first leak might be tolerable, but subsequent attacks using this leaked information pose a high-impact risk.

Brand monitoring involves activities aimed at achieving comprehensive surveillance of an organisation's digital footprint, covering the dark web, deep web, and surface web. Similar to dark web monitoring, any attack indicators identified through brand monitoring ensure early detection of potential threats, breaches, fraud, and illicit use of intellectual property.

Web as we (or do not) see it



Key Challenges

- Leaked accounts or compromised devices can lead to further exposure, disclosure of sensitive data, or an outage.
- Lack of awareness regarding data leaks or compromised accounts.
- The growing online environment increases organisations' exposure to reputation threats and unauthorised use of sensitive data.
- Many organisations find it challenging to monitor their digital presence across various and constantly evolving online platforms.
- Negative mentions, misinformation, and brand impersonation can damage trust, revenue, and market share.
- Unauthorised use of company resources can weaken identity and cause legal issues.

Cynode's Dark Web & Brand Monitoring service addresses the following use cases:

1)Dark Web Intelligence

2) Brand Monitoring

- Corporate Credential Leak
- Third-party Credential Leak
- Compromised Devices
- Sensitive Data Disclosure
- Fake Social Media Accounts
- Phishing Monitoring

Main Benefits

Comprehensive Coverage & Visibility:
Ensures no aspect of your digital presence is overlooked and delivers an overarching view of the organization's digital exposure.
Proactive Defence & Risk Mitigation:
Enables businesses to stay ahead of cybercriminals with real-time alerts and actionable intelligence. Dramatically reduces the risk of breach at the outset.
Operational Efficiency:
Frees up internal resources from complex monitoring tasks.

Dark Web Intelligence

Cynode's Ultima Cyber Threat Exposure Platform:

- monitors hacker discussions, marketplaces, channels, and other malicious platforms to detect any sensitive information, hacking activities, and exploit trading related to our customers, and assesses their severity and credibility.
- performs manual review and verification of the exposure within the dark web source and conducts a thorough investigation to identify the impacted assets of our customers.
- assesses the potential risks posed by past breaches and exposed data, considering factors such as sensitivity, volume, and potential for misuse or exploitation by threat actors.

Cynode responds strategically and swiftly to mitigate risks with the following essential actions:

- taking immediate steps to contain the exposure of sensitive data on the dark web, such as requesting takedowns of illicit postings.
- sending notifications to alert security teams about any mentions or indications of our customers' compromised data on the dark web.

Corporate Credential Leak

The service identifies leaked credentials (usernames and passwords) associated with our customers' domain names by monitoring the dark web, forums, botnets, and other sources. Leaked credentials pose significant risks as these accounts could be registered, authorised, and used for logging into the organisation's public and internal applications, remote access systems, device sign-ins, and email access.

Cynode evaluates each leaked credential by validating the account's current password and usage status. The credential incidents are prioritised and triaged based on factors such as source and extent of the leak, details in the intelligence, password validation results and the resources that these accounts are registered and authorised. Following this step, Cynode provides the necessary response to mitigate the risk. The response may include one or more of the following actions:

- Enforce password reset
- Revoke current sessions
- Block or limit account access
- Enforce multi-factor authentication
- Disable account temporarily

Third-party Credential Leak

Our service identifies non-corporate credentials that may have been leaked from both public and internal applications hosted under our customers' domain names. These credentials are registered, authorised, and used for logging into any B2B or B2C applications within our customers' networks.

Cynode analyses third-party credential leaks to determine the asset responsible for the leak. These credentials might be found on compromised devices connected to a botnet or infiltrated from the organisation's assets. We identify the source and method of the leak and respond with appropriate actions, which may include:

- Blocking or limiting access from compromised devices
- Revoking current sessions for employee accounts on compromised devices
- Notifying the relevant organisation contact with recommendations to:
  - Enforce a password reset for third-party accounts
  - Isolate the asset related to the leak
  - Limit access to the asset related to the leak

Compromised Devices

The service identifies devices compromised by a botnet, evaluates their relevance to our customers' existing environment, and the potential risk posed by the data exposed on these compromised devices. These devices are either part of an organisation's domain and/or have corporate accounts logged in. Compromised devices can potentially expose sensitive information, including employee, personal and third-party credentials, intellectual property, and financial data and files. Cynode responds with actions relevant to the type of exposed data.

Sensitive Data Disclosure

Cynode conducts an immediate assessment to determine the scope, nature, and severity of the data disclosure incident, including the type of sensitive data involved, how it was exposed, and the potential impact on affected individuals and the organisation. The disclosed data could potentially affect an organisation's finances, market position, or reputation.

Cynode notifies the relevant customer contacts and verifies the authenticity and accuracy of the disclosed sensitive data through cross-referencing.

Fake Social Media Accounts

Cynode verifies the authenticity of suspected fake or fraudulent accounts by comparing them against official accounts and brand guidelines, checking for inconsistencies in branding, content, and engagement patterns.

Cynode initiates taking down action against malicious actors who created and are operating fake or fraudulent accounts by collaborating with social media platforms and industry organisations.

Phishing Monitoring

Cynode's phishing monitoring includes:

- Assessment of DNS records related to the newly registered domains and reference web pages to identify any targeted phishing campaigns and fraudulent web content.
- Performing manual review and verification of newly registered domains that match or closely resemble the organization's legitimate domains, checking for inconsistencies or suspicious indicators.
- Conducting regular WHOIS lookups to gather information about newly registered domains, including registrant details, registration date, name servers, and domain registrar, to assess their legitimacy and potential threat level.

Cynode provides proactive blocking and mitigation of similar or look-alike domains with the following actions:

- Providing feed lists includes indicators like domains, URLs, and mail server addresses. This allows the organization to block mail delivery or prevent user access to fraudulent content.
- Notify relevant stakeholders about the detection of new similar or look-alike domain registrations, enabling coordinated response and action.
- Submit domain take-down requests to domain registrars, hosting providers, or domain abuse reporting platforms for unauthorised or malicious domains, following established procedures and guidelines.

Ready to safeguard your digital presence and stay ahead of cyber threats?

Partner with Cynode to leverage our comprehensive Dark Web & Brand Monitoring services. Gain unparalleled insights, proactive defences, and actionable intelligence to protect your organisation from potential breaches, data leaks, and malicious activities. Contact us today to learn more about how we can help you maintain a secure and resilient digital footprint.

CYNODE PROACTIVE HARDENING SERVICES