ManageEngine
Log360

Dark web monitoring:

Protecting your data in the shadows

Introduction to **dark web monitoring**

The dark web is a hidden part of the internet where cybercriminals often trade stolen information, such as personal data, financial details, and login credentials.

By monitoring the dark web, you can scan these hidden networks for specific data like personal identifiable information (PII) and sensitive business information. When such data is detected, you can take immediate action to protect your organization's assets and prevent further damage.

Types of data monitored

Dark web monitoring tracks various types of sensitive information and potential threats, including, but not limited to:

PII

Names, addresses, social security numbers, passport numbers, and other personal data that can be used for identity theft.

Financial information

Credit card numbers, bank account details, login credentials for financial accounts, and other financial data that could be exploited for fraud or unauthorized transactions.

Intellectual property (IP)

This includes leaks of proprietary business information, trade secrets, copyrighted material, and other intellectual property that could be misused or sold illegally.

Exposed credentials

Usernames, email addresses, and passwords for various online accounts, which could be used for unauthorized access or account takeovers.

Threat intelligence

Any discussions, activities, and indicators of potential cyberthreats, such as malware, ransomware, hacking tools, and exploit kits, providing organizations with warnings of those potential dangers to bolster their cybersecurity defenses.

How dark web monitoring works

Dark web monitoring leverages specialized techniques to proactively safeguard your personal information from the hidden corners of the internet. Here's a breakdown of its core functions:

Crawling

Custom software traverses the complex dark web landscape, identifying relevant forums, marketplaces, and other potential data repositories.

Data extraction

Extracted content from these locations is then processed and analyzed for specific data points.

Matching and alerting

Advanced algorithms compare the extracted data against your PI, including domains, email addresses, usernames, and social security numbers. If a potential match is identified, you'll receive a prompt notification.

ManageEngine
Log360

Log360's dark web defense

Log360 utilizes a comprehensive strategy to safeguard your organization from dark web threats:

24/7 dark web monitoring

Log360 leverages real-time threat data from Constella Intelligence, a leading provider of dark web insights, empowering you to stay constantly updated on the latest threats lurking in the dark web.

Active threat scanning with Vigil IQ

Log360's powerful threat detection engine, Vigil IQ, utilizes the acquired threat intelligence to actively scan your network for indicators of these identified threats. This proactive approach spots attacks before they can gain a foothold.

Comprehensive threat visibility

Log360 goes beyond basic detection. By providing a clear and comprehensive view of all dark web threats, including botnet leaks, you can take preventive action before threats escalate.

Incident workbench for in-depth investigation

When a potential threat is flagged, Log360's Incident Workbench gathers and analyzes contextual data, providing valuable insights into the threat's history and potential impact.

Real-time alerts

Log360 keeps you informed every step of the way. You'll receive immediate alerts whenever a potential threat, like leaked credentials or exposed information associated with your domain, is identified in the dark web. This allows you to take swift and decisive action to mitigate the potential impact.

Proactive threat mitigation

Following threat identification and investigation, Log360 empowers you to take proactive measures to mitigate these threats. This includes actions to address vulnerabilities within your organization and supply chain that could be exploited by threats.

ManageEngine
Log360

Proactive threat mitigation with Log360

Log360 utilizes a comprehensive strategy to safeguard your organization from dark web threats:

Automated incident response

Design custom workflows with a drag-and-drop interface to mitigate cyberattacks effectively.

Data leak prevention (DLP)

Spot unusual file or data accesses using ML-based UEBA to detect abnormal user behavior.

Threat intelligence integration

Retrieve the latest threat information from reliable feeds and monitor your network for potential threats.

Unified security data analysis

Seamlessly gather security data from various sources, including AD users, network devices, and applications like vulnerability scanners and DLP software.

Want to see how Log360 monitors the dark web for leaked information?

Talk to our experts

About Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, an analytical Incident Workbench, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoringcapabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

$ Get Quote

Download