RISK COGNIZANCE

DARK WEB
Monitoring

involves the use of specialized tools and techniques to proactively scan hidden and unindexed parts of the internet to identify potential security threats such as data leaks, stolen credentials, and other forms of cyber risks.

Automated Threat Detection:
Dark web monitoring uses ML, NLP, and web crawlers to detect exposed credentials, sensitive data, and insider threats in real time, triggering alerts for high-priority risks.

Integrated Response and Mitigation Plans:
Detected threats are categorized by severity and linked to predefined response steps, with integration into SIEM, SOAR, and collaboration tools to ensure efficient mitigation.

Detailed Threat Reports:
Regular reports summarize risks, sources (e.g., dark web forums), and potential impacts like account takeovers or phishing, helping teams prioritize and allocate resources.

Proactive Detection and Prevention:
Early detection of risks, such as leaked credentials, prevents larger breaches and informs security improvements, like enhanced access controls and phishing training.

Continuous Improvement:
Insights from monitoring strengthen cybersecurity strategies, improve threat preparedness, and ensure regulatory compliance and alignment with industry standards.

sales@riskcognizance.com

www.riskcognizance.com