DRPS Solution Brief

Digital Risk Protection Services

Continuous Monitoring of Open and Dark Web Sources to Identify Threats

Digital Risk Protection Services (DRPS) refers to a set of cybersecurity practices that provides holistic safeguarding for an organization's digital assets. It is designed to identify, monitor and mitigate digital risks including threats to an organization's financial health, brand reputation or customer trust. DRPS covers vital cybersecurity practices including threat intelligence gathering, data analysis to identify risks with automated and manual monitoring techniques in order to ensure the safety of digital assets while sustaining a secure environment. The solutions under DRP services aim to detect, track and analyze threats in real-time while using the advantage of having threat intelligence data and developing AI algorithms.

Digital Risk Protection

Since digital transformation has become an emerging issue globally, it is vital for organizations to embrace DRPS features to protect their brand reputation, minimize financial losses and improve customer trust. Cyber attacks can disrupt the organizational operations, leading to reputational damage or pose a significant risk to financial balances which can take years to recover. Also DRPS are quite crucial for social media platforms too which lead to damage to the brand reputation of an organization, as these platforms are increasingly targeted by cyber criminals aiming to steal personal credentials, spread misinformation and conduct other malicious attacks.

Emerging technologies have made it possible for threat actors to carry out fraudulent activities like data theft, money laundering and phishing scams via online platforms and tools. Organizations need to adopt strong anti-fraud /cybersecurity practices to detect and mitigate outcoming risks.In the pursuit of unmasking potential fraudulent activities targeting a specific enterprise, SOCRadar leverages its advanced ML-powered fraud detection capabilities through comprehensive surveillance of a myriad of digital channels used by threat actors. This includes not just traditional platforms like websites, but also extends to social media platforms, clandestine dark web forums, and exclusive online marketplaces. SOCRadar's XTI platform utilizes cutting-edge tools like machine learning, and data analytics to find trends and abnormalities that could be indicators of fraud attempts.

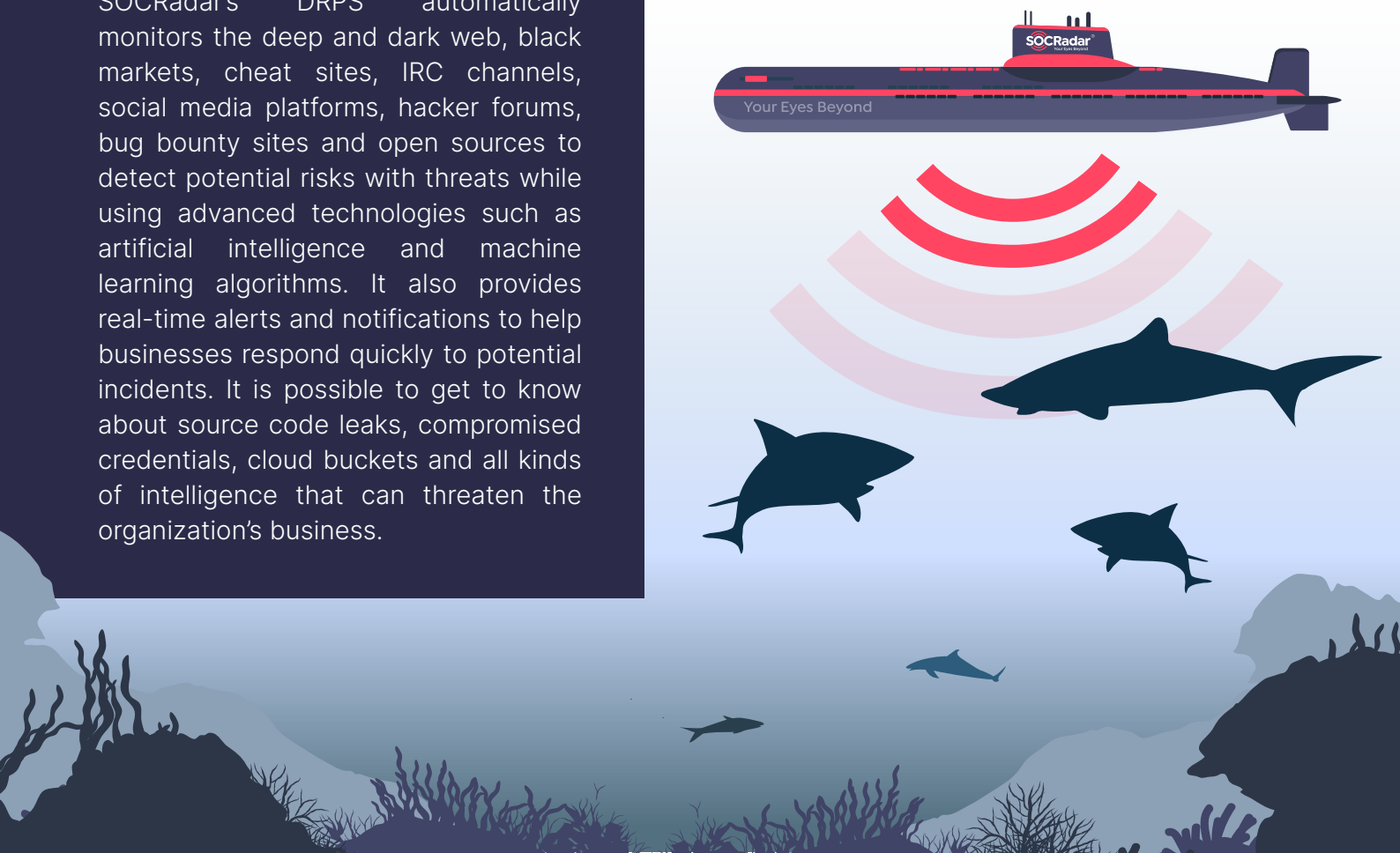
SOCRadar's DRPS

Stay One Step Ahead Of Threat Actors With Actionable Intelligence Alerts

SOCRadar's Digital Risk Protection Services under Extended Threat Intelligence (XTI) helps businesses to proactively manage their digital risks, protect their reputation, safeguard their critical assets and data. It prioritizes helping organizations mitigate digital risks and protect their sensitive data and assets while allowing them to be prepared for all kinds of threats from the open, deep and dark web. DRPS typically include technologies like threat intelligence, monitoring and analysis tools, and incident response services, all designed to ensure the safety of the digital assets and minimize the outcoming threats.

SOCRadar's DRPS solution is built on instant phishing domain identification, dark web and compromised credential detection skills by aggregating and correlating massive data points into actionable intelligence alerts. With the power of DRP services, SOCRadar offers a range of features and tools to help businesses manage their digital risks effectively. These include risk assessment and scoring, threat intelligence feeds, incident response workflows, and collaboration and reporting tools. It provides comprehensive coverage for various types of digital risks, including brand infringement, data leaks, cyber threats, and more. The DRPS module enables an organization's Security Operations and Risk Management teams to swiftly and effectively understand how particular risks they may face and what to do for mitigation. The module aims to empower teams like fraud and law, in order to protect their brand from being discredited, legal trouble and the intellectual property falling into the hands of malicious actors.

SOCRadar's DRPS automatically monitors the deep and dark web, black markets, cheat sites, IRC channels, social media platforms, hacker forums, bug bounty sites and open sources to detect potential risks with threats while using advanced technologies such as artificial intelligence and machine learning algorithms. It also provides real-time alerts and notifications to help businesses respond quickly to potential incidents. It is possible to get to know about source code leaks, compromised credentials, cloud buckets and all kinds of intelligence that can threaten the organization's business.



DRP services of SOCRadar have the ability to crawl, analyze and interpret data with monitoring a wide variety of dark web layers and to identify data exposures and malicious activities in advance. The analyzed data sets from huge dumps of compromised credentials, data leakages, torrents, exploits, stolen credit card information, posts in dark web forums about hacking tools and campaigns.

DRPS

SOCRadar's DRPS crawling algorithms can help SOC teams to spot and address social media threats in real-time giving them the added visibility. The machine learning algorithms help to analyze user behavior and identify patterns that may indicate a potential threat on social media platforms such as Twitter, Facebook and Instagram are considered to be more than a regular communications platform with billions of users. Threat actors frequently benefit from social media's popularity by abusing it for cybercrime, fraud, phishing, impersonating and proliferation of misinformation causing brand reputation losses.

In the rapidly enlarging environment of digitalization, SOCRadar's DRPS module is designed to help to safeguard both individuals and businesses from the potentially devastating consequences of cyber threats. With providing real-time alerts and actionable intelligence to help organizations mitigate these risks before they become major issues, SOCRadar's DRPS aims to carry the security environment to the cutting-edge.