
PROACTIVE RISK MANAGEMENT

PARM



POWERED BY



SOVEREIGN
INTELLIGENCE



SOLVING FOR “X” - *WE KNOW WHERE TO LOOK*
High-fidelity Data Meets Artificial Intelligence

2017

MISSION

To provide commercial and government entities smarter understanding of threats from external and internal sources through the application of deep-learning artificial intelligence and high-fidelity data from otherwise inaccessible domains so that risks to cyber, financial, brand, and enterprise integrity are quickly identified and mitigated.

BACKGROUND

Proactive Risk Management (PARM) is a worldwide, leading edge, strategic, security and risk management consulting company focused on providing tailored solutions to address the problems of our clients. We take great pride in providing flexible, precise, and actionable information, as well as full-service turnkey projects in a timely manner. PARM is unique in the field of security management in that it has elected to forge business alliances with leading industry specialists worldwide as opposed to trying to be everything to everyone.

Proactive Risk Management has access to some of the brightest and most experienced professionals in the intelligence field, both domestically and internationally. Our Human Intelligence staff is supplemented by PARM's forefront cyber tools and strategic partners. In addition, we can support combining Social Media, Dark Web and Internet monitoring with powerful forensic analysis to establish a greater understanding of the problem at hand. Our proven capabilities save time and resources, directly protecting the integrity of any project.

Sovereign Intelligence is a worldwide computer software company with premium consultancy offerings. Established to address the two pillars of sound multinational business: (1) Reconnaissance and (2) Cognition. We are the world's only full spectrum cyber radar technology that survey's Surface, Social Media, Dark Web, and Peer-2-Peer global file sharing networks to detect and thwart threats to privacy, intellectual property, assets, and reputation.

Through its strategic partnership with Sovereign Intelligence, PARM helps clients *Solve for X* so that they can understand the threat environment and make informed critical decisions.



Contact Us

www.parminc.com

ProActive Risk Management Inc.
900 South Figueroa Street, Suite 3005
Los Angeles, CA 90015
+1-213-840-8856 Office
+1-888-511-0908 Toll Free
+1-877-744-2637 24/7 Emergency

info@parminc.com

SOLUTIONS

CYBER



Threat intelligence is more than just understanding network security vulnerabilities. It's about understanding who is involved and how they operate. The prevention of cyber threats begins by addressing enterprise data to detect and attribute weaknesses. We answer these questions for multinationals and government agencies by analyzing our proprietary library of hidden data of dark web forums and peer-to-peer networks.

External Threats

Sophisticated cyber criminals are typically driven by financial gain or varying adherence to an idea, (i.e. "hackivism"). Understanding the 'why' has led us to look for evidence of external threats within the dark web. As the functionality of The Onion Router (TOR) affords a reasonable modicum of anonymity; dark web forums, IRC channels, and invite-only sites are an enticing medium for nefarious behavior. However Sovereign's Reconnaissance platform goes much further. By integrating and organizing social media, deep web public records and peer-to-peer domains, we are able to provide our clients with a single view of their external threats. Sovereign's use of deep learning enables more valuable exploration and indexing of large unstructured data sources, while enriching the analysis. The result is real-time finished intelligence.

Internal Anomalies

It is now possible to understand sentiment and analyze for patterns of behavior and intent by analyzing petabytes of unstructured data -including files, emails, video, and network logs - from a single platform. Sovereign Cognition integrates, organizes, and analyzes any structured

or unstructured data within your enterprise data to find the real anomalies that pose actual threats.

Attribution

The Sovereign team has spent many years working within the US intelligence community. We know that cyber security companies often fail to provide the context of who is behind an attack, or who has perpetrated the fraud. Attribution of a threat is important for considering legal options and provides a means to understand and ultimately deter the criminal from attacking again. Our deep learning AI captures and corroborates personally identifiable information (PII) used to profile criminals and linked associates across external and enterprise data sets to provide detailed target intelligence.

Forensics

When multinationals are breached, the scene of the crime often consists of evidence that is scattered around the globe. Critical evidence is discovered among incongruent forms, including emails, IP logs, internet browser history, leaked files, and other unstructured data sets where no clear pattern exists. Acquisition and organization is important for the integrity of the investigation. The Sovereign Cognition platform helps examiners integrate, tag, log, and analyze information in real time, thus enhancing live acquisition and evaluation in accordance with relevant IOS/IEC standards.

Case Study: Cyber Security Redux. Combining Carding Script Attribution with Global Forensics

FINANCIAL



The financial world is replete with case studies for those who myopically address the current wave of cyber crimes. Without a coherent strategic plan to either learn which data sets within the enterprise are causing problems, or learn about where threats are originating from outside their networks, today's financial institutions are doomed to the "bolt-on vendor" approach. Sovereign brings holistic solutions to derive wisdom from data. We build custom workflows that effortlessly interact with an AI to help lower risk, improve performance and streamline operating costs.

AML/KYC

As anti-money laundering regulations seek increased consistency, firms are wisely taking a holistic approach to the way they manage their risk. Sovereign uses deep learning and sophisticated intelligence techniques to improve fraud detection, reduce false positives and automate key workflows. Knowing your client has become as difficult as knowing your vendors. Our KYC solution automatically queries against any sophisticated databases such as social media, deep web public records, dark web and peer-to-peer domains. This approach saves time and resources by analyzing potential red-flags in realtime.

Due Diligence

Failure to conduct serious due diligence investigations results in significant fines. Leaving unknown financial accounts and unreported affiliations to chance is like playing Russian roulette. We can help. During Merger & Acquisition transactions, our Due Diligence solutions help integrate internal data sources with our proprietary data to

deliver automated checks for any entity - like finding the needle in a haystack.

Market Insights

Emerging markets, regulatory fluctuations, evolving industry trends, and untapped data sets make investment decisions difficult and expensive. Sovereign allows you to plug in any kind of real-time, static, proprietary or public unstructured data collections to surface non-obvious data insights and reveal potential alpha-generating signals.

Compliance

Compliance with new regulations such as the Foreign Corrupt Practice Act and UK Bribery Statute are wreaking havoc on unsuspecting firms struggling to quickly understand their enterprise weak links. The current process of manually conducting background checks of third-party consultants is failing. Our compliance solutions automate and customize any workflow to reduce human error and streamline manual efforts involved in compliance with the FCPA, FCA, CCAR, DFAST or Basel-III frameworks.

Case Study: Financial Fraud Prevention.

SI Reconnaissance Uncovered \$40 Million Global Fraud Scheme. See www.sovereign.ai.

BRAND



The need to protect your company's most valuable brand assets and marketing strategies has never been more important in the presence of growing sophisticated cyber threats. Working closely with government and companies in any industry, the Sovereign team of intelligence experts leverage your data, our AI platform and proprietary data collection techniques to shine a light on the darkest corners of the web to identify and mitigate real or perceived threats to key business assets.

Intellectual Property

From patents to bespoke workflows, Sovereign works closely with multinationals in any industry to identify and thwart potential threats to intellectual property. This includes connecting internal security data (e.g. logs, sensors, emails) with proprietary dark web and peer-to-peer data collection techniques. The results is a radically new way to either assess historical threats or proactively thwart them.

Market Sentiment

What customers perceive is often more important than reality. The question is which data sets will provide the best understanding of market sentiment. Sovereign Cognition helps our clients understand customer sentiment, via emails, social media, recorded phone complaints, and so on. Whether identifying or predicting non-obvious industry trends or organizing enterprise data, Sovereign's AI helps clients model market sentiment quickly with powerful deep learning tools.

Reputation

Shareholders increasingly expect companies to protect their brand reputation. Understanding where to start in order to assess the current sentiment of the customer base

is difficult. Current trends to apply over-engineered social media feeds are beginning to fail because those intent on harming a company's reputation initiate their conspiracies in forums like the dark web, peer-to-peer networks, and encrypted messaging applications. Sovereign Reconnaissance integrates these non-traditional data sets with its deep learning AI in order to identify potential risks.

Fraud

Fraud comes in many forms and increasingly happens over the Internet. Sovereign identifies real threats by integrating your enterprise data with the continuous monitoring of the dark web and peer-to-peer networks where nefarious activities are more likely to exist. Sovereign's deep learning AI quickly supports investigative efforts to find fraudulent behavior patterns for analysis.

Geopolitical

Protests, environmental issues, political disasters, terrorism, state collapse or crisis, failure of national governance, and interstate conflict are just a few of the geopolitical risks we monitor in support of our clients' security. We collect and use information gathered from indigenous news sources, geographically referenced activities, satellite imagery, global human sources, governments, online communications and climate reports to assess global hot spots and produce in-depth analysis on these issues. By alerting on geopolitical imminent threats, we enable clients to react to crises while continually monitoring to identify long-term trends.

ENTERPRISE



Identifying risks, fraud and bottlenecks often starts by exploring data with questions that are not always well-defined. The Sovereign Cognition platform provides a collection of tools for the exploration of data, detection of non-obvious patterns and trends, and dynamic visualization for data analysis. These tools make it possible to tackle a number of challenges present in any of today's large enterprises and often relegated to bespoke IT projects. Explore your data collections with unprecedented ease, power and flexibility.

Physical Assets

Protecting physical assets involves a sophisticated, holistic approach to understanding threats from cyber or internal operators. Sovereign's Cognition and Renaissance platforms make it possible to combine both internal and external data sources deemed critical to the integrity of corporate assets. Integrating and organizing this data under one platform makes it possible to observe, predict, and ultimately mitigate otherwise unknown threats to the business.

Supply Chain

Proprietary methodologies in every company's supply chain are under threat by internal actors, industry competitors and even other countries. Sovereign's Cognition platform helps companies understand their supply chain exposure, by mapping and organizing logistical data, vendor profiles, and unstructured shipping data, etc. We can help uncover the weak links often overlooked until its too late.

PII/PHI

Personally identifiable information (PII), or personal health information (PHI), is used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context, (i.e. sensitive health records). Safeguarding this information from identity thieves is critical to sustaining the integrity of insurance companies, human resources departments, accountancies, and healthcare providers. Sovereign is able to quickly integrate sensitive profiles and monitor for anomalies and predatory activities across the Internet.

Insider Threat

The growing concern of internal operators requires a new approach to identify and mitigate threats from within an organization. Today's employees often have unprecedented access to sensitive data not intended for public consumption. Sovereign's Cognition platform will help identify anomalies among internal data sets as well deliver attribution for threats outside the network.

Case Study: Finding the Insider Threat. Identifying Malware Conspiracies Originating in the Dark Web. See www.sovereign.ai.