SOVEREIGN INTELLIGENCE

Sovereign Intelligence

REAL WORLD APPLICATIONS

SOVEREIGN.AI

We solve the toughest problems for the best organizations in the world with Real Intelligence.

Mission

Founded in 2014 by attorney and former clandestine intelligence officer, Mark Johnson, Sovereign is staffed by Silicon Valley veterans, US & UK intelligence engineers, analysts, and operators. Our DNA invites extraordinary curiosity, rigorous integrity, and the relentless pursuit of excellence. We help solve the problem of weak decision-making, whether instigated by siloed data, inadequate intelligence collection, biased AI assumptions, or stymied sense-making.

The number #1 reason the best organizations in the world chose Sovereign: Experience. As former clandestine intelligence officers we:

- Know where to look to solve tough problems
- Operate with Diligence, Precision & Integrity.

Intelligence experts have long considered the measurement of device location to be the holy grail of intelligence collection, e.g. the missing link for predictive analysis and the number one method for saving costs when it comes to learning about where people are, yesterday, today, and tomorrow.

Sovereign Intelligence Solutions

We pride ourselves in diligently solving tough problems for our clients. We have programs to help deliver our solutions: (1) Investigative Intelligence, (2) Artificial Intelligence, and (3) Location Intelligence.

Investigative Intelligence

Sovereign has been solving tough problems for the best organizations in the world. As an elite team of former intelligence officers and cyber analysts we efficiently answer questions related to cyber threats, security breaches, financial fraud, and influence operations. We know where to look and we move fast. Check our our Applications below to see what we've accomplished.

Artificial Intelligence

Our proprietary AI solutions address the problem of weak decision-making, whether instigated by siloed data, inadequate intelligence collection, biased AI assumptions, or stymied sensemaking capacity. Our AI solutions amplifie the innate capabilities of Intelligence Analysts, accelerating predictive analysis, enhancing confidence, and answering real-world questions.

Location Intelligence

Why Location Intelligence? Location Intelligence provides you insight into population movement on a global scale. Location Intelligence helps to generate leads, reduce costs, and uncover footfall trends. At Sovereign, we observe 16 Billion global location events everyday. These events include mobile device geolocation movement. With global insight into device movements, the sky is the limit toward generating predictive analytics for Marketing, Real Estate investment, Retail, Traffic Flow, or Executive Travel Protection.

Cyber Intelligence

Card Script Attribution

Background

In 2016, a global European payment processing company engaged Sovereign Reconnaissance to monitor Dark Web and other salient sites for potential extraneous vulnerabilities. With millions of customers and merchants relying upon seamless account access, network continuity is paramount. Identifying trends of cyber criminals hijacking customer login scripts for card-testing would pose a tremendous burden on internal network security, diverting resources, ultimately jeopardizing brand confidence.

Challenge

Two major issues arose once Sovereign Reconnaissance identified original card-testing scripts targeting the company,: was the company establishing a reputation as a reliable card testing venue and whether attribution of the culprits was viable?

Result

Sovereign's 24/7 monitoring was deployed with automatic tripwires to capture and index sites posing threats to the client. The tripwire service alerted to the threat of an original card testing script targeting the client's customer identification credentials. Over a dozen profiles were quickly established across multiple internet domains. The detailed profiles were organized by pseudonym, time of postings, ontology, sentiment, motivation, and risk. While those details would have sufficed to demonstrate the growing reputation hazards facing the client, an unusual foreign carding site was discovered, creating the necessity for further *attribution*. Sovereign's forensic team immediately established links between a BitCoin blockchain and a foreign merchant, ultimately providing the site's full transaction details, as well as the merchant's contact information for further fraud notification. Sovereign additionally scanned server banners from the original web server, metadata from the page source, and the Google UID, via our proprietary Reconnaissance search engine, extracting critical information from the foreign ISP. Sovereign ultimately discovered the original ISP and IP of the carding site. The client successfully altered critical components of their network security as a result.

Insight

Alerting multinational transaction companies that card testing is underway only solves part of the problem. Combining Dark Web monitoring with powerful forensic analysis in- house to establish greater understanding of the problem and attribution saves time and resources, directly protecting the integrity of the organization.

Cyber Intelligence

Insider Threat Attribution

Background

In 2016, a global European payment processing company engaged Sovereign Reconnaissance to monitor Dark Web and other salient sites for potential extraneous vulnerabilities. With millions of customers and merchants relying upon seamless account access, network continuity is paramount. Identifying trends of cyber criminals hijacking customer login scripts for card-testing would pose a tremendous burden on internal network security, diverting resources, ultimately jeopardizing brand confidence.

Challenge

Two major issues arose once Sovereign Reconnaissance identified original card-testing scripts targeting the company,: was the company establishing a reputation as a reliable card testing venue and whether attribution of the culprits was viable?

Result

Sovereign's 24/7 monitoring was deployed with automatic tripwires to capture and index sites posing threats to the client. The tripwire service alerted to the threat of an original card testing script targeting the client's customer identification credentials. Over a dozen profiles were quickly established across multiple internet domains. The detailed profiles were organized by pseudonym, time of postings, ontology, sentiment, motivation, and risk. While those details would have sufficed to demonstrate the growing reputation hazards facing the client, an unusual foreign carding site was discovered, creating the necessity for further *attribution*. Sovereign's forensic team immediately established links between a BitCoin blockchain and a foreign merchant, ultimately providing the site's full transaction details, as well as the merchant's contact information for further fraud notification. Sovereign additionally scanned server banners from the original web server, metadata from the page source, and the Google UID, via our proprietary Reconnaissance search engine, extracting critical information from the foreign ISP. Sovereign ultimately discovered the original ISP and IP of the carding site. The client successfully altered critical components of their network security as a result.

Insight

Alerting multinational transaction companies that card testing is underway only solves part of the problem. Combining Dark Web monitoring with powerful forensic analysis in- house to establish greater understanding of the problem and attribution saves time and resources, directly protecting the integrity of the organization.

Financial Intelligence

Financial Fraud

Background

In 2016, a global European payment processing company engaged Sovereign Reconnaissance to monitor Dark Web and other salient sites for potential extraneous vulnerabilities. With millions of customers and merchants relying upon seamless account access, network continuity is paramount. Identifying trends of cyber criminals hijacking customer login scripts for card-testing would pose a tremendous burden on internal network security, diverting resources, ultimately jeopardizing brand confidence.

Challenge

Two major issues arose once Sovereign Reconnaissance identified original card-testing scripts targeting the company,: was the company establishing a reputation as a reliable card testing venue and whether attribution of the culprits was viable?

Result

Sovereign's 24/7 monitoring was deployed with automatic tripwires to capture and index sites posing threats to the client. The tripwire service alerted to the threat of an original card testing script targeting the client's customer identification credentials. Over a dozen profiles were quickly established across multiple internet domains. The detailed profiles were organized by pseudonym, time of postings, ontology, sentiment, motivation, and risk. While those details would have sufficed to demonstrate the growing reputation hazards facing the client, an unusual foreign carding site was discovered, creating the necessity for further *attribution*. Sovereign's forensic team immediately established links between a BitCoin blockchain and a foreign merchant, ultimately providing the site's full transaction details, as well as the merchant's contact information for further fraud notification. Sovereign additionally scanned server banners from the original web server, metadata from the page source, and the Google UID, via our proprietary Reconnaissance search engine, extracting critical information from the foreign ISP. Sovereign ultimately discovered the original ISP and IP of the carding site. The client successfully altered critical components of their network security as a result.

Insight

Alerting multinational transaction companies that card testing is underway only solves part of the problem. Combining Dark Web monitoring with powerful forensic analysis in- house to establish greater understanding of the problem and attribution saves time and resources, directly protecting the integrity of the organization.

Financial Intelligence

Bank Compliance Risk

Background

A global, US-based, investment bank engaged Sovereign Intelligence to develop a risk monitoring dashboard to make sense of emerging compliance risks. Typically a holistic endeavor in today's compliance departments, the bank understood that tracking emerging risks could be automated with the help of Sovereign's artificial intelligence algorithms and processes. It worked with Sovereign to configure it's platform to pull in anything from regulator speeches, state attorney general offices, social media and internal communications and fed them into an interactive charting engine. The result was a radically new, analytics-driven approach to a practice area typically oriented around manual effort.

Challenge

Two major issues arose once Sovereign's began configuring its platform for the needs of the bank. First, a handful of data sources required subscription access or did not provide programmatic access via API or RSS/XML feeds to easily retrieve source data. We were able to address this by periodically downloading new content. The second was working closely with the bank to develop a charting style, with the right level of abstraction, that made sense for the team interacting with it on a regular basis. Easily customizable and flexible, we worked to tune the application to uncover the right emerging threats from the underlying data sets.

Result

Managing global compliance risk in these modern times has grown increasingly more difficult for today's risk agents. Not only are there simply more sources to cover, but the scrutiny from various governing bodies has never been higher. More than ever before, risk analysts need a reliable computer-based, decision-support system that relies on AI and algorithms to assist risk agents to make (or predict) recommendations. Sovereign's Compliance Risk solution addresses this need. In collaboration with the bank's risk analysts, Sovereign ingested and indexed all of the relevant, real-time data sources which were then plotted on an interactive chart by risk type, recency and threat level. The results was a real-time engine constantly making decisions and displaying real- time emerging risks for further dissemination by the compliance risk team – saving thousands of hours of manual time to achieve much of the same goal, while shining a brighter light on areas that can severely impact the firm.

Insight

Compliance risk teams often have to translate a complex, holistic process into one that is more analytical in nature Quantifying potential risks with the Sovereign platform does that while enabling a more thoughtful way for management to make sense of real or perceived threats to its business.

Brand Intelligence

Loyalty Program Fraud

Background

A multinational European hoteling chain sought aid safeguarding a points-based loyalty program that offers a variety of benefits for continued use of the brand's hospitality services.

Challenge

The chain hired Sovereign to support this goal by monitoring and investigating potentially fraudulent actors. Like many global hospitality chains, the company had been a frequent topic of discussion in underground forums, darknet marketplaces, and other black market communities.

Result

Sovereign uncovered a secret online community of cyber criminals who were actively selling, discussing, and distributing illicit access to loyalty program members' accounts, thus allowing the theft of points which could be used to buy room nights or converted to buy airline tickets and e-vouchers from major online retailers. Access to members' accounts also provided access to certain categories of personally identifiable information (PII.) Sovereign identified multiple criminal actors within this community, including one who had illicitly gained access to loyalty club accounts, some with balances of over 100,000 points. We engaged the criminal actor and gleaned key intelligence regarding fraudulent activity threatening the company, including the modus operandi used to compromise the accounts

Insight

In today's global marketplace, the hospitality industry is particularly exposed to complex and ambiguous risks in an increasingly technology-driven world. Loyalty and rewards points programs often walk hand-in-hand with a greater digital footprint, which can also mean greater exposure of sensitive data such as credit card details and other personally identifiable information.

Brand Intelligence

Fake Pharmaceuticals

Background

The tide of fake pharmaceuticals has risen to incomprehensible levels. In early 2016, one of the most recognizable pharmaceutical brands in the world, with $70 billion USD in revenue, began addressing their concerns by exploring tactics used by cyber criminals to promulgate the distribution of falsified drugs. The specific drug at issue: *a controversial stimulant used for the treatment of Attention- Deficit Hyperactivity Disorder (ADHD)*. With market share and liability issues involved with the unregulated commerce of this drug, understanding the threats to its global brand became critical.

Challenge

The questions poised to Sovereign were how prevalent is the black market industry regarding this specific stimulant, and whether any attribution to the major dealers was realistic. Understanding the metrics involved and damage to the company's reputation through expensive survey's and general Social Media analysis already proved to be inefficient.

Result

Although the prevalence of eCommerce sites within the Dark Web offering hacking tools, malware, and credit cards, is substantial, the market for counterfeit drugs dwarfs them all. Sovereign's proprietary search engines and Artificial Intelligence were engaged to determine the effect of fake pharmaceuticals on the company's brand. SI Reconnaissance integrated our data feeds from the Dark Web, Deep Web forums, and other sensitive sites requiring social engineering. Sovereign quickly found salient data points including URLs, pseudonyms, email addresses, addresses, and even telephone numbers of otherwise unknown black market dealers selling this stimulant. Completing the overall picture with Surface and Social Media data, Sovereign successfully determined that the counterfeit sale of this particular drug did not have a profound effect on the companies overall reputation.

Insight

Understanding whether your reputation is damaged by counterfeit products sales is important in averting brand diminishment and thus loss of market share. Sovereign's vast cataloging of unstructured Dark Web market intelligence provided invaluable data points for the company's strategic plans to dismantle counterfeit products.

Brand Intelligence

Ride-Sharing Fraud

Background

A global ride-sharing company enlisted Sovereign's services to identify threat actors attempting to defraud its drivers for free rides. Like many of its peer ride sharing apps, the company has been a frequent topic of discussion in underground forums, darknet marketplaces, and encrypted messaging applications.

Challenge

A leading dark web business intelligence firm originally hired to address the problem failed to gain critical insight into dynamic channels used to communicate the malicious algorithms amongst the originating bad actor community involved.

Result

Sovereign acquired intelligence derived from deep diver investigation of bar-to-entry encrypted messaging channels. This intelligence was paired with real time, on-the-ground investigative work aimed at illuminating the step- by-step processes of fraudulent ride acquisition. As a result, Sovereign not only uncovered a variety of illicit resellers populating dark web forums; active threat actors were also identified across multiple chat platforms. Due to a comprehensive, multi-tiered intelligence-gathering and analytic process, we identified threat actors at all stages of the fraud process, including resellers, active customers, and potential customers, as well as fraud guides that unveiled the process by which scams were enacted.

Initial estimated losses for the company reached nearly $200,000 per week. Within a short time frame, SI provided the critical intelligence necessary to secure the company's internal platform. **These measures reduced the loss to $20,000 per week, netting approximate savings for the company of $720,000 per month.**

Insight

In today's global marketplace, app-based car sharing services face unique risks in an increasingly technology-driven world. Because they are primarily web-dependent applications, these types of businesses often boast a greater digital footprint, which also enables greater exposure of sensitive data such as credit card details and other personally identifiable information. Such exposure makes these companies prime targets for fraud schemes. By combining proprietary machine learning techniques with cyber-strategic know-how and experience in law enforcement investigation techniques, SI has devised multiple means to counter cybercrime.

Influence Intelligence

Social Network Exploitation

https://www.reuters.com/article/us-facebook-brazil-election

Background

A Silicon Valley social media giant fell prey to a coordinated misinformation campaign based in Brazil that used false social media profiles to strategically and deliberately mislead the public regarding the Brazilian political landscape.

Challenge

Two major issues arose once Sovereign Reconnaissance identified original card-testing scripts targeting the company,: was the company establishing a reputation as a reliable card testing venue and whether attribution of the culprits was viable?

Result

The company enlisted Sovereign to investigate the parties responsible for the misinformation campaign, as well as their tactics, techniques, and procedures (TTPs). In response, we acquired intelligence derived from full scope searches of the Internet, including deep and dark web spaces. This investigative strategy was implemented over the course of several weeks. As a result, we ultimately uncovered the identities and methods of several actors behind the political misinformation movement.

One group in particular produced the illusion of curating its messaging through multiple independent news outlets by misrepresenting shared control of social network pages. This method allowed them to lend their fraudulent information a false sense of authenticity. However, through a rigorous multi-tiered investigative process, SI was able to identify not only fake and misleading profiles, but also their creators. As such, the client was able to deactivate 196 pages and 87 accounts in Brazil ahead of the October 2018 elections.

Insight

The modern geopolitical landscape increasingly finds itself subject to misinformation campaigns conducted over popular social media networks. The rise of increased online social networking creates a ripe environment for fake news actors, social media fraudsters, and other nefarious individuals to sow dissent and spread false messaging for their own ends.

Sovereign Intelligence
1775 Tysons Blvd. 5th Floor
McLean, VA 22102
discover@sovereign.ai
sovereign.ai

McLean I San Fransisco I London I Tokyo