ID Force Cybersecurity

and Dark Web Monitoring

Technical Specification for Dark Web Monitoring

1. A comprehensive cybersecurity solution aimed at enhancing threat intelligence, detection, and prevention capabilities against ransomware, cyber threats, and criminal activities on the deep and dark web. The solution will provide real-time intelligence, facilitate collaborative intelligence sharing, and will comply with relevant regulations and standards.
2. Solution Overview:
3. Real-Time Threat Intelligence:
4. Provision of real-time intelligence on active cyber threat groups.
5. Dynamic updates on emerging threats at a fraction of the cost of static intelligence reports.
6. National Security Enhancement:
7. Ability to set up actor and keyword alerts to defend against supply chain attacks, critical infrastructure threats, and destabilizing ransomware.

8. Threat Intelligence Access:
9. Access to indexed data from marketplaces, forums, and leak sites, spanning a minimum of 15 years.
10. Access to both public/open and closed/private forums, marketplaces and Telegram channels. Where possible and available, provide access to restricted areas of sites hidden behind reputation locks or similar mechanics.
11. Deep and Dark Web Visibility:
12. Secure access to deep and dark web criminal communications without risking the safety of cybersecurity teams or infrastructure.
13. Capability to navigate a comprehensive dataset of clear, deep, and dark web sources securely.
14. Collaborative Intelligence Sharing:
15. Secure data sharing capabilities to deconflict targets across multiple investigations with partner agencies.
16. Facilitate improved cyber posture by providing actionable insights into threat groups for better offensive and defensive actions.
17. Provide a case management system to collect relevant information, facilitate the sharing of information between team members and external relevant parties.
18. Prevention and Detection:
19. Illumination of deep and dark web threats and prevention of cyber attacks by leveraging intelligence gathered from dark web data.
20. Proprietary technology for monitoring dark web traffic without requiring installation of agents.
21. Access to a virtual machine for secure and simplified access to Tor and I2P onions.
22. Provide safe and anonymous access to TOR browser on live data
23. Automated data collection and analysis capabilities, utilizing advanced AI and analytics to proactively alert against imminent threats.
24. Capability to proactively discover, add and index new data sources to support further intelligence requirements
25. Assist with translation of foreign language materials, with priority given to those languages most common on the dark web

26. Provide a full audit trail, enabling monitoring of staff actions
27. Identification of when data was collected (i.e sourced/ scraped) and from where
28. Case/ report management functionality to enable collection of information of interest
29. Ability to export data saved into case management/ reporting functionality
30. Graphical User Interface (GUI) makes it easy to navigate and user friendly
31. Application Programming Interface (API) is accessible for integration with 3rd party systems
32. Users will be able to build complex queries to identify specific information of interest amongst the complete dark web data set, which will include, but not be limited to Boolean logic queries
33. An index of archived and existing dark web sites will be available, providing users a cached/ offline view of how the site appears
34. Ransomware groups will be monitored, giving users an insight into their activity.
35. User/ threat actor activity will be aggregated for dark web actors to include history, themes, similar profiles and unique OSINT e.g. PGP keys and email addresses
36. Dashboards will provide users insights into the data being collected, shared, discussed or sold across multiple areas of collection, i.e within a specific market
37. Users will be able to set alerts for query matches varying in frequency from real time to a weekly summary
38. Ability to deconflict activity, enabling team leads to manage cross-over investigations
39. Unique identifiers shared by users will be extracted from the collected data to allow investigation to pivot from specific data points. Unique identifiers will include, as a minimum; emails, phone numbers, IP Addresses, CIDR, PGP Public Key Fingerprints, MAC Addresses and crypto address, i.e Bitcoin and Litecoin.

Administration:

1. Enable multiple teams to be created and managed by a manager/ administrator
2. User profile creation, editing and deletion by manager/ administrator
3. Granular controls over user’s access to specific features within the capability
4. Comprehensive logging and audit functionality, which should include, but not be limited to; case audit logging, user audit log and organisational audit log
5. Password reset mechanisms should exist for users to self-serve password resets
6. Two Factor Authentication should be utilised across user accounts
7. Additional, ad hoc training sessions should be offered to support user understanding and feature/product releases, where required

Compliance and Certification:

1. The solution complies with industry standards and regulations related to cybersecurity and data privacy - including ISO27001, Cyber Essentials, SOC2 and similar
2. Certifications or accreditations demonstrating the solution's effectiveness and reliability in combating cyber threats are available if required.

Delivery and Implementation:

1. The solution is easy to deploy throughout the organization without requiring extensive setup or configuration.

2. A clear timeline will be provided for deployment and implementation, including pre-launch training, mid-year business reviews, and post-launch support and growth exploration.
3. Users will be able to access the tool from any laptop/PC, providing they have a reliable internet connection and active user credentials.
4. Users will be provided with documentation to support familiarity and onboarding, which will include at least User Guides and Quick Start Guides.

Warranty and Training :

1. License is valid for 36 months including Certified Training, support and maintenance.
2. Where required, training should be delivered to relevant teams, covering an introductory session, as well as more advanced sessions.

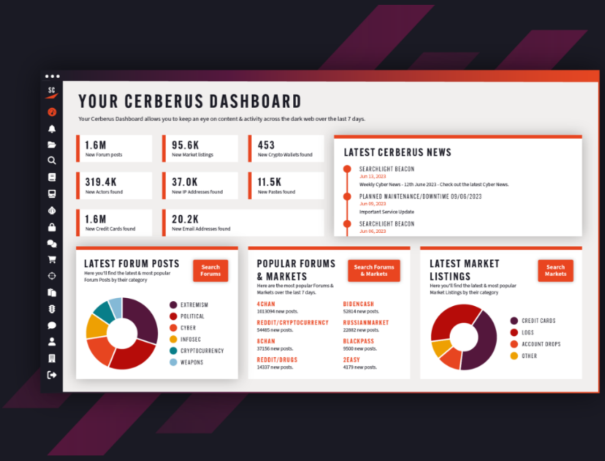
PRODUCTS

CERBERUS: DARK WEB INVESTIGATION

A powerful investigation platform and comprehensive dark web database for uncovering criminal activity on the deep and dark web.

CRIMINALS USING THE DARK WEB THINK YOU CAN'T SEE THEM, WITH CERBERUS YOU CAN

Cerberus uses proprietary techniques developed by world-leading researchers to deliver the most comprehensive dark web database on the market, providing access to intelligence that was previously unobtainable.



YOUR CERBERUS DASHBOARD

Your Cerberus Dashboard allows you to keep an eye on content & activity across the dark web over the last 7 days.

1.6M New Forum posts

95.6K New Market listings

453 New Crypto Wallets found

319.4K New Actors found

37.0K New IP Addresses found

11.5K New Pastes found

1.6M New Credit Cards found

20.2K New Email Addresses found

LATEST CERBERUS NEWS

SEARCHLIGHT BEACON
Jun 13, 2023
Weekly Cyber News - 12th June 2023 - Check out the latest Cyber News.

PLANNED MAINTENANCE/DOWNTIME 09/06/2023
Jun 09, 2023
Important Service Update

SEARCHLIGHT BEACON
Jun 06, 2023

LATEST FORUM POSTS

Here you'll find the latest & most popular Forum Posts by their category

POPULAR FORUMS & MARKETS

Here are the most popular Forums & Markets over the last 7 days.

4CHAN
1013094 new posts.

BIDENCASH
52814 new posts.

REDDIT/CRYPTOCURRENCY
54485 new posts.

RUSSIANMARKET
22882 new posts.

8CHAN
37156 new posts.

BLACKPASS
9500 new posts.

REDDIT/DRUGS
14337 new posts.

2EASY
4179 new posts.

LATEST MARKET LISTINGS

Here you'll find the latest & most popular Market Listings by their category

TRUSTED DARK WEB DATABASE

OUR DARK WEB DATA IS TRUSTED GLOBALLY BY LAW ENFORCEMENT AND GOVERNMENT AGENCIES

PROVEN DARK WEB DATA

The world's leading analysts and investigators use Cerberus to keep their people and countries safe online. It has been used in some of the biggest cases involving dark web activity and has had a proven impact in bringing perpetrators to justice.

INTUITIVE INVESTIGATION

Cerberus is designed to reduce labor for enterprise teams, law enforcement and government agencies. It does not require technical skills, background or knowledge to use and allows your people to investigate dark web data without putting themselves at risk or having to download any special software.

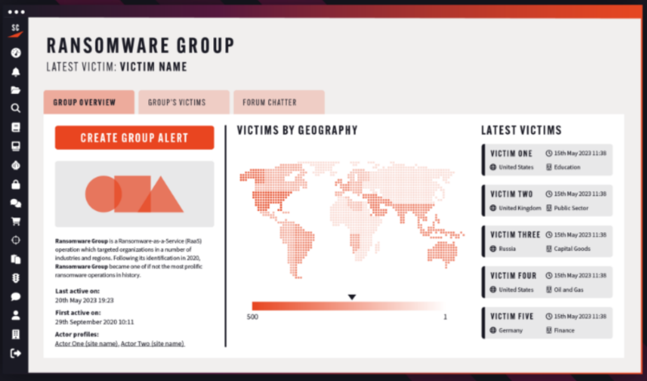
EVIDENTIAL DATABASE

Our case management features enable you to maintain, audit, and report on multiple investigations across multiple teams. Automated alerting, reporting, and sharing of resources means that cases can be built in real-time and the ability to collaborate across departments within the platform means that you can easily deconflict targets.

RANSOMWARE AND DARK WEB SEARCH TOOL

GATHER THREAT INTELLIGENCE ON RANSOMWARE GROUPS

Ransomware continues to be one of the greatest concerns for governments and security professionals alike. The Cerberus Ransomware Search and Insights module helps investigators gain the advantage on ransomware groups with access to continuously updated intelligence on their latest tactics, known members, and victims.



RANSOMWARE GROUP

LATEST VICTIM: **VICTIM NAME**

Ransomware Group is a Ransomware-as-a-Service (RaaS) operation which targeted organizations in a number of industries and regions. Following its identification in 2020, **Ransomware Group** became one of if not the most prolific ransomware operations in history.

Last active on:
20th May 2023 19:23

First active on:
29th September 2020 10:11

Actor profiles:
Actor One (site name), Actor Two (site name)

VICTIMS BY GEOGRAPHY

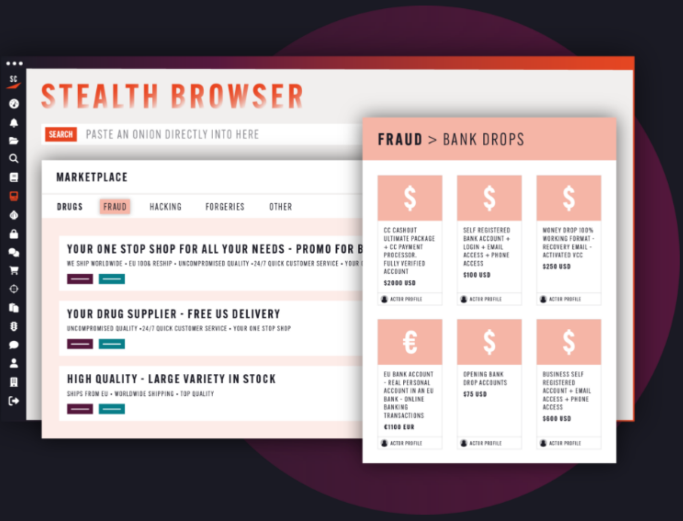
LATEST VICTIMS

VICTIM ONE	United States	15th May 2023 11:38 Education
VICTIM TWO	United Kingdom	15th May 2023 11:38 Public Sector
VICTIM THREE	Russia	15th May 2023 11:38 Capital Goods
VICTIM FOUR	United States	15th May 2023 11:38 Oil and Gas
VICTIM FIVE	Germany	15th May 2023 11:38 Finance

STEALTH BROWSER

YOUR VIRTUAL MACHINE TO ANONYMOUSLY INVESTIGATE THE DARK WEB

The dark web is a critical source of data and intelligence for cybersecurity professionals, but accessing it carries risks for the investigator and their organization. Stealth Browser eliminates these risks by automatically masking the investigator's digital fingerprint, allowing investigators to quickly and securely access Tor and I2P onions on the dark web without risk to themselves or their organization's infrastructure.



YOUR ONE STOP SHOP FOR ALL YOUR NEEDS - PROMO FOR B

WE SHIP WORLDWIDE • EU 100& RESHIP • UNCOMPROMISED QUALITY •24/7 QUICK CUSTOMER SERVICE • YOUR

YOUR DRUG SUPPLIER - FREE US DELIVERY

UNCOMPROMISED QUALITY •24/7 QUICK CUSTOMER SERVICE • YOUR ONE STOP SHOP

HIGH QUALITY - LARGE VARIETY IN STOCK

SHIPS FROM EU • WORLDWIDE SHIPPING • TOP QUALITY

CC CASHOUT ULTIMATE PACKAGE + CC PAYMENT PROCESSOR. FULLY VERIFIED ACCOUNT
$2000 USD

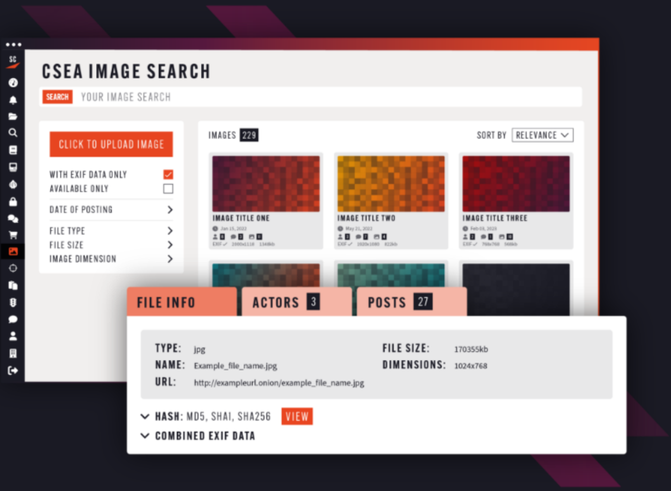
SELF REGISTERED BANK ACCOUNT + LOGIN + EMAIL ACCESS + PHONE ACCESS
$100 USD

MONEY DROP 100% WORKING FORMAT - RECOVERY EMAIL - ACTIVATED VCC
$250 USD

EU BANK ACCOUNT - REAL PERSONAL ACCOUNT IN AN EU BANK - ONLINE BANKING TRANSACTIONS
€1100 EUR

OPENING BANK DROP ACCOUNTS
$75 USD

BUSINESS SELF REGISTERED ACCOUNT + EMAIL ACCESS + PHONE ACCESS
$600 USD



TYPE: jpg
NAME: Example_file_name.jpg
URL: http://exampleurl.onion/example_file_name.jpg
FILE SIZE: 170355kb
DIMENSIONS: 1024x768
HASH: MD5, SHAI, SHA256

CSEA IMAGE SEARCH

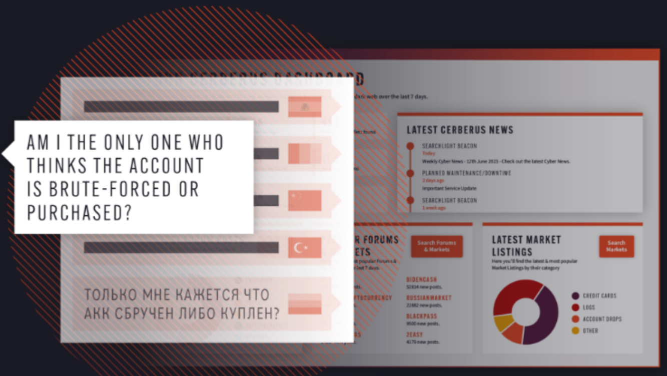
IDENTIFY VICTIMS OF CHILD SEXUAL EXPLOITATION. PROSECUTE OFFENDERS.

Provide your law enforcement officers with access to our intuitive CSEA image search. Regardless of their dark web experience, they can search by keyword, image metadata, or image upload to gather evidence on high-risk actors.

AI-POWERED LANGUAGE TRANSLATION

MAKE SEARCHING ON THE DARK WEB EASIER

Instantly translate data in the top 10 languages used on the dark web, including Russian, Chinese, and French. Searchlight translates full sentences as accurately as a human using Neural Machine Translation (NMT) and has been trained to understand Russian dark web slang – so you can decipher what criminals are really saying.



AM I THE ONLY ONE WHO THINKS THE ACCOUNT IS BRUTE-FORCED OR PURCHASED?

ТОЛЬКО МНЕ КАЖЕТСЯ ЧТО АКК СБРУЧЕН ЛИБО КУПЛЕН?

dark web over the last 7 days.

SEARCHLIGHT BEACON
Today
Weekly Cyber News - 12th June 2023 - Check out the latest Cyber News.

PLANNED MAINTENANCE/DOWNTIME
2 days ago
Important Service Update

SEARCHLIGHT BEACON
1 week ago

Here you'll find the latest & most popular Market Listings by their category

BIDENCASH
52834 new posts.

RUSSIANMARKET
22882 new posts.

BLACKPASS
9500 new posts.

2EASY
4179 new posts.

DARK WEB DATA SOURCES

DEEPEST DARK WEB DATABASE

Cerberus creates a mirror image of the dark web so your teams can safely navigate the most comprehensive database of clear, deep, and dark web sources. Investigate live sites or search back through more than 15 years of historic dark web data.

MITIGATE THE RISKS OF ACCESSING DARK WEB DATA

Extracting data from the dark web is challenging and dangerous. There are many risks for organizations or enforcement teams who access the dark web without using Cerberus, including malware, trojans, and phishing attacks. Cerberus mitigates these risks by hiding your digital footprint, which means investigators can search dark web data, safe in the knowledge that their identity is protected and malware can’t jump to their organization’s live network.

HOW DO WE SOURCE OUR DARK WEB DATA?

Searchlight Cyber gathers data from different sources on the dark web, including underground forums, marketplaces, and encrypted chats, using automated and manual techniques. Our threat intelligence team has a wealth of experience in law enforcement, cybercrime, and the military. We utilize advanced tools such as cutting-edge web crawlers and natural language processing to extract context-rich information from dark web data.

DARK WEB DATASET BENEFITS

CONDUCT INVESTIGATIONS USING DARK WEB DATA

UNCOVER THE CYBERCRIMINAL UNDERWORLD

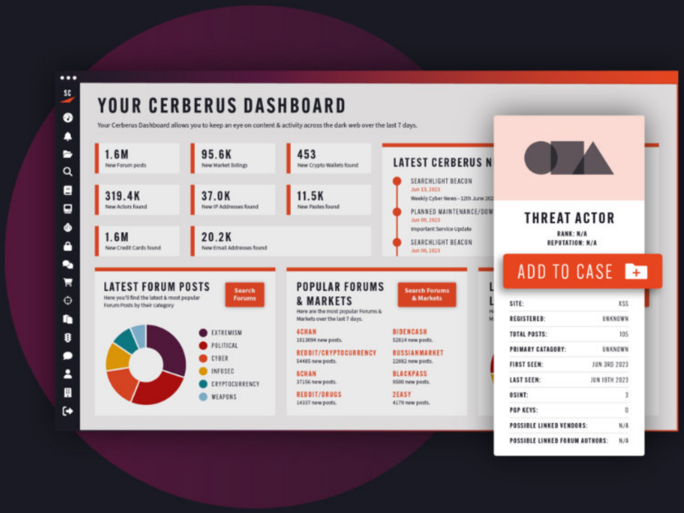
Understand the scale of criminal activity on the dark web to inform resourcing and investigation.

TRACK ILLEGAL COMMODITIES

Gain visibility into the sale of credentials, vulnerabilities, malware, drugs, arms, child exploitation materials, and more on dark web marketplaces.

IDENTIFY ACTORS

Investigate individuals and groups with the ability to pivot on usernames, aliases, and historic activity.



YOUR CERBERUS DASHBOARD

Your Cerberus Dashboard allows you to keep an eye on content & activity across the dark web over the last 7 days.

1.6M
New Forum posts

95.6K
New Market listings

453
New Crypto Wallets found

319.4K
New Actors found

37.0K
New IP Addresses found

11.5K
New Pastes found

1.6M
New Credit Cards found

20.2K
New Email Addresses found

LATEST CERBERUS N

SEARCHLIGHT BEACON
Jun 13, 2023
Weekly Cyber News - 12th June 202

PLANNED MAINTENANCE/DOW
Jun 09, 2023
Important Service Update

SEARCHLIGHT BEACON
Jun 06, 2023

LATEST FORUM POSTS

Here you'll find the latest & most popular Forum Posts by their category

POPULAR FORUMS & MARKETS

Here are the most popular Forums & Markets over the last 7 days.

4CHAN
1013094 new posts.

REDDIT/CRYPTOCURRENCY
54485 new posts.

8CHAN
37156 new posts.

REDDIT/DRUGS
14337 new posts.

BIDENCASH
52814 new posts.

RUSSIANMARKET
22882 new posts.

BLACKPASS
9500 new posts.

2EASY
4179 new posts.

THREAT ACTOR

RANK: N/A
REPUTATION: N/A

SITE:	XSS
REGISTERED:	UNKNOWN
TOTAL POSTS:	105
PRIMARY CATAGORY:	UNKNOWN
FIRST SEEN:	JUN 3RD 2023
LAST SEEN:	JUN 19TH 2023
OSINT:	3
PGP KEYS:	0
POSSIBLE LINKED VENDORS:	N/A
POSSIBLE LINKED FORUM AUTHORS:	N/A

EXTRACT THREAT INTELLIGENCE

Uncover the activity of cybercriminals in the pre-attack phase, to inform cyber defenses.

REPORT ON DARK WEB ACTIVITY

Powerful reporting features within the platform allow you to meaningfully share findings with other teams or senior leadership.

GATHER DIGITAL FORENSICS

Build case files of evidence gathered from your investigations into activity on the clear, deep, and dark web.

Contact info@idforce.io

ID Force International Pty Ltd
Suite 705, 11 Railway Street
Chatswood NSW 2067
Sydney, Australia