PROTECTIVE
INTELLIGENCE

CERBERUS®
THE DARKNET INTELLIGENCE TOOL

USER-FRIENDLY INTERROGATION OF THE
WORLD'S LARGEST DARKNET DATA SET

INTRODUCTION
DARKNET THREATS

The darknet, and specifically Tor, is designed to keep users anonymous by shielding their true IP addresses behind a Tor IP address. Users can either browse the open web or hidden services.

Hidden services are frequently used for selling stolen databases, hosting command & control servers for botnets, ransom pages and other nefarious activity. Tor can also be used to launch attacks on networks via the internet, without exposing their true origin.

There are many ways for criminals to profit from exploiting vulnerabilities in network systems.

Malicious software can hijack machines into being bots in their network and use them for mining crypto-currency, stealing sensitive data, spreading malware and participating in cyber-attacks.

CYBER SECURITY
HEADLINE FIGURES

Average cost of a data breach — **$18.28m**

Increase in cost per breach in 5 years — **↑62.5%**

Growth of data breaches in 5 years — **↑300%**

Darknet search % for illegal material — **65%**

Number of darknet users per day — **2million+**

SEE IN THE DARK **WITH CERBERUS®**

Criminals using the darknet think that you can't see them. But with CERBERUS® you can!

CERBERUS® is the world's most comprehensive darknet intelligence platform. Using our web-based portal you can safely monitor an otherwise secretive and complex part of the internet, and react to potential cyber threats to your organisation.

With no software to be installed on your network and no operational disruption, Cerberus® has been designed to be used without the need for any technical training. The interface will feel familiar to anyone that uses a mobile phone or web browser.

CERBERUS® 10 KEY BENEFITS

01 **Easy to use web-based platform**

02 **No software to install on your network**

03 **Safely search darknet services offline**

04 **Monitor outside hacking attempts and internal threats**

05 **Know when your data is being sold or distributed on the darknet**

06 **Filters remove malicious scripts and images**

07 **Explore darknet forum posts**

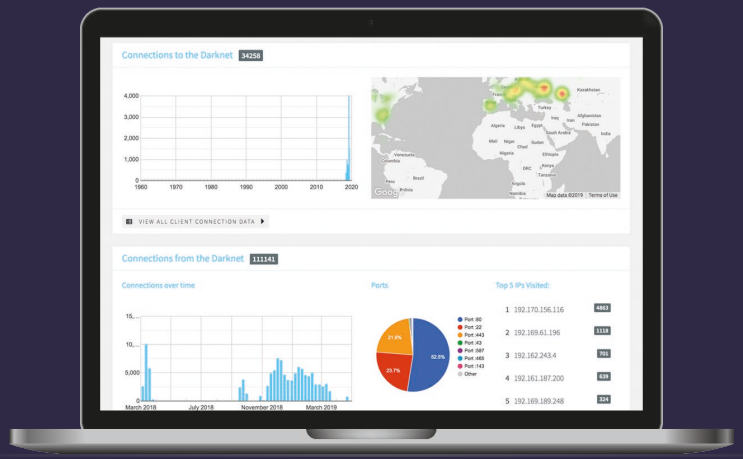
08 **Receive instant alerts of suspicious activity**

09 **Save content to exportable case files and share with colleagues**

10 **Investigate, track and gain insights using sophisticated analytics**

CERBERUS®
FEATURE SET

Using proprietary techniques developed by world leading researchers, CERBERUS® goes deeper than crawlers alone. A comprehensive dataset indexes and stores darknet content, monitors traffic and provides insight in to this hidden world.



SEARCH

DARKNET SEARCHING

Safely search and navigate the darknet without installing any special software on your network.

HIDDEN SERVICES

The world's most comprehensive database of hidden services. Easily search and browse without compromising operations security.

OSINT DATABASE

Comprehensive index of emails, IP addresses, bitcoin wallets and other open source intelligence.

MONITOR

DARKNET MARKETS

Search and monitor an ever-growing network of darknet marketplaces and darknet vendors.

DARKNET TRAFFIC LOGS

Monitor network activity across multiple networks and domains, and receive alerts for specific traffic activity.

DARK FORUM MONITORING

Monitor specific bad actors and explore their networks, activity profiles and posts.

ANALYSE

CONTEXTUAL ANALYSIS

Use meta data and analytics to gain sophisticated insights and contextual understanding of darknet activity.

DARKNET ARCHIVE

Archive of historical darknet pages allows you to search for compromising data that may have since been removed or modified.

TREND MONITORING

Monitor high level trends on the darknet to understand the big picture and provide context.

MANAGE

CASE MANAGEMENT

Maintain, audit and report on multiple investigations across multiple teams.

ACTIVITY ALERTS

Alerts can be set on keyword searches, network traffic, markets, forums or OSINT. Customise alert intervals to your requirements.

PASTE MONITORING

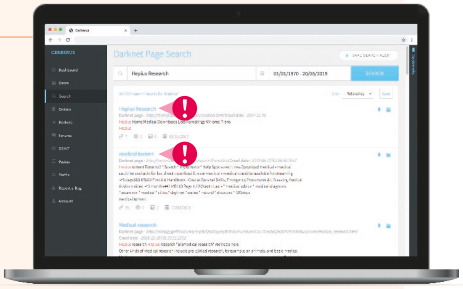
Monitor darknet and clearnet paste-bins for leaked credentials and security breaches.

CASE STUDY
CYBER SECURITY

The following hypothetical case study shows the steps by which Cerberus® can be used to help protect your assets from darknet users and malware within your organisation.

Hepius Research Plc. is at risk from hackers and malicious insiders. Hepius Research performs medical research and holds confidential information as well as valuable trade secrets that are coveted by other companies and governments. You have to help secure their latest project, 'Panacea'.

01. THE INVESTIGATION BEGINS

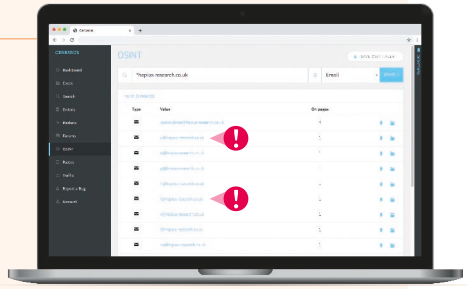


You open a new case for Hepius Research.

You search the darknet for 'Hepius Research' and 'Panacea', saving results to your case and creating new activity alerts.

Search the darknet safely and securely with Cerberus®. Easily create alerts for relevant keywords.

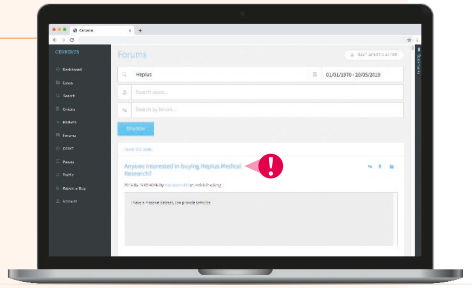
02. DISCOVERING LEAKS



You search for OSINT related to Hepius Research employees and domains, getting multiple positive hits.

Cerberus® has one of the world's largest searchable databases of darknet OSINT.

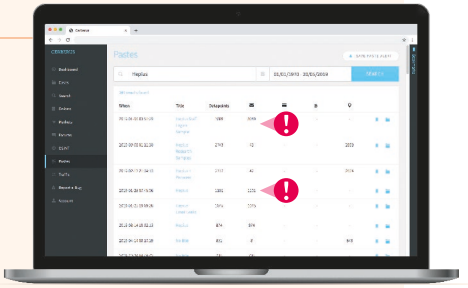
03. TRACING THE LEAKS



Exploring darknet forums has confirmed your suspicions. Panacea is being discussed by Hacktivists.

Cerberus® provides a simple interface for searching darknet forums and users.

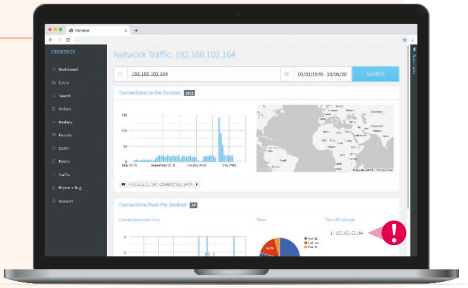
04. INVESTIGATING THE LEAKS



A paste bin search has revealed leaked email addresses and passwords of Panacea researchers.

Cerberus® indexes darknet and clearnet paste bins for easy searching of leaked data.

05. A SUSPECT IS IDENTIFIED



Searching darknet traffic logs reveals the IP address of a disgruntled employee attempting to sell sensitive data.

Cerberus® has exhaustive logs of darknet traffic, helping you to identify suspicious behaviour.

06. CASE CLOSED

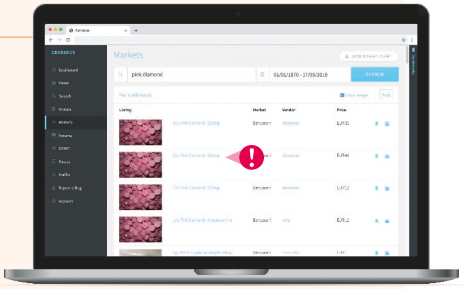
You pass the details on to Hepius Research and law enforcement.

CASE STUDY
LAW ENFORCEMENT

With a full suite of analytics to measure macro and local trends, Cerberus® provides powerful insights into darknet criminality. Navigate the darkweb offline to avoid leaving a footprint and store your case information on-premises behind your firewall, to keep all case data confidential.

A new drug, Pink Diamond, *has infiltrated London and caused deaths amongst party goers. It is unknown where the drug is coming from, but the suspicion is that it is being bought in bulk on the darknet.*

01. THE INVESTIGATION BEGINS

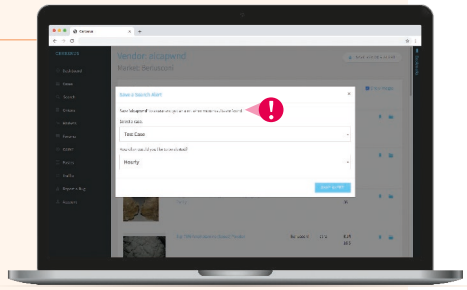


You create a new case in Cerberus®

You search the darknet and the darknet markets for *Pink Diamond* saving all hits to you case file.

Cerberus® allows you to search the darknet and darknet markets without compromising operational security.

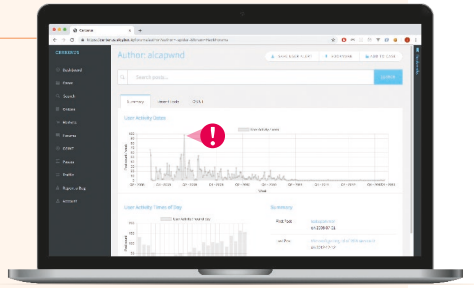
02. DISCOVERING LEAKS



You find a darknet vendor called 'SkyHye' selling large quantities of *Pink Diamond*. You create an alert to track their activity.

Cerberus® alerts allow you to stay up-to-date with bad-actor activity.

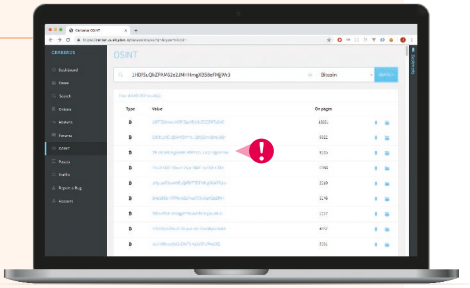
03. INVESTIGATING VENDORS



The Vendor forum profile reveals a pattern of posting habits, indicating a European timezone.

Cerberus® collects meta-data that provides valuable context to your investigation.

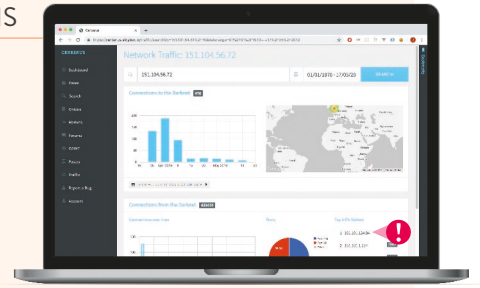
04. FOLLOWING THE MONEY



OSINT captured from the market listings reveals a bitcoin wallet hash that is known to have purchased class-A drugs.

Cerberus® indexes bitcoin wallet hashes and helps you reconcile them to bad-actors.

05. ANALYSING TRAFFIC PATTERNS



You cross-reference the IPs of suspected local drug dealers with darknet traffic metrics. One traffic pattern matches the posting profile.

Cerberus® traffic analysis is an essential tool for identifying bad-actors in the real world.

06. TAKING ACTION

You raid the address, discovering a large cache of *Pink Diamond*. The arrest is made.

CERBERUS®
ADDITIONAL FEATURES

Using proprietary techniques developed by world leading researchers, CERBERUS® goes deeper than crawlers alone. A comprehensive dataset indexes and stores darknet content, monitors traffic and provides insight into this hidden world.

We have developed an intricate knowledge of the darknet and a powerful tool-set that can be used to enhance CERBERUS®. We recognise that there is not a single silver bullet for cyber security. To fully protect a system requires a full arsenal.

SOC API INTEGRATION

FINE TIME RESOLUTION

The API will monitor your network at a higher time resolution for darknet traffic. Gain a better understanding of volume and the timing of connections. This allows for the detection of traffic spikes and greater analysis.

SCALABILITY

The API feed can be scaled to suit your budget and requirements.

INTEGRATION

Integrate our darknet feed into your operations centre or dashboard keeping all your feeds in one place.

MORE ALERTS

The number of alerts is limited in Cerberus® cases. The API allows for a much greater number of alerts and queries to be run.

DIGITAL FORENSIC SERVICES

CUSTOM REPORTING

We can build automated custom darknet reports and dashboards tailored to your requirements.

OPERATIONAL SUPPORT

Our team of darknet experts are available to support your law enforcement operations and investigations.

FORENSIC TOOLS

Our development experts will work with you to deliver a custom and powerful solution to fit your requirements.

BESPOKE INTEGRATION

Our experts can build APIs and analytics to integrate with your systems and processes.

CERBERUS®
NEXT STEPS

To arrange a demonstration or for more information, simply get in touch

EMAIL

info@protectiveintelligence.co.uk

PHONE

+44 (0)1869 247814

Protective Intelligence brings together a group of security specialists who all have a passion for delivering high-quality solutions to our clients.

We believe that the challenge is to move Information Security into the heart of the organisation, where everyone understands the importance of protecting data from loss, corruption or exposure.

Our experience ranges over five continents, with clients located in a wide range of countries.

We are adept at providing the best Information Security & Protection advice, from corporate giants to charities, secure government departments to local councils, and from the heart of New York and London to the streets of Mozambique and Kabul.

THE CORNER HOUSE
24 NORRIS ROAD
UPPER ARNCOTT
BICESTER
OXFORDSHIRE
OX25 1NZ

+44 (0)1869 247814
info@protectiveintelligence.co.uk

protectiveintelligence.co.uk