DarkMAP
Web Intelligence

CatchProbe **DarkMAP** is not just a simple platform where you can feed on intelligence information. It brings you to the forefront of next-generation defense technologies with its strong analysis capabilities, data enrichment, and infrastructure driven by artificial intelligence.

One objective of **DarkMAP** is to enable exploration and indexing across all layers of the Internet: Social Media, DeepWeb, and DarkNet. DarkMap can archive the targeted pages without missing any content and has the ability for automated content tracking and discovery processes.

Another differentiating factor of **DarkMAP** from other WEBINT products is its fast setup, low cost, and the ability to escalate and delegate tasks among analysts and departments. Additionally, **DarkMAP** presents the collected content in a functional, simple, and comprehensive manner, enabling analysts to effortlessly conduct their research.

Features:

- Threat group association through keyword analysis
- Blind spot detection on the dark net using iterative link analysis
- Flow management feature for membership-requiring platforms like forums, IRC groups, and Telegram groups
- Multilingual resources translated into English.
- Real-time threat analysis
- Crime and criminal analysis with cross-case analytics insights using CrimeGround
- Low-cost and high-efficiency with SaaS infrastructure

Overview

Tree Branch Methodology

Unique Technology

SaaS Based Platform

Easy to Use

AI and Next-Gen Analysis

Proactive Defense Capabilities

IOC and threat discovery using regular expressions

Attacker analysis facilitated by WebInt platform

Event-based risk analysis for analysts

Escalation and delegation process for analysts

Detailed authorization protocols among departments and analysts

GAIN SPEED & TIME

GET CRITICAL INSIGHT

FIND EMERGING THREATS

EXPLORE THE DEEP

OTD BİLİŞİM
GLOBAL VAD

DARKMAP: NAVIGATING THE DIGITAL DEPTHS

SURFACE WEB

INTEL COLLECTION EFFORT: MINIMAL

Web scraping tools, search engine API's and OSINT techniques

TYPE OF INTEL FOUND

All publicily available information

DEEP WEB

INTEL COLLECTION EFFORT: MODERATE

Data extraction from APIs, databases or password-protected environments.

TYPE OF INTEL FOUND

- Corporate and government databases
- Subscription-based research or news sites
- Intranets or organizations

VALUE

Offers valuable, exclusive information such as private discussions.

DARK WEB

INTEL COLLECTION EFFORT: HIGH

May involve social engineering, linguistics expertise and ethical hacking.

TYPE OF INTEL FOUND

- Stolen credentials and credit card numbers
- Cybercrime toolkits (malware, ransomware)
- Illicit marketplaces (drugs, weapons, counterfeit goods)

VALUE

- Essential for organizations concerned about data breaches or illicit transactions.
- Can reveal upcoming cyberattacks, vulnerabilities being sold or new criminal trends.

ANONYMOUS NETWORKS (TOR, I2P, YGGDRASIL)

INTEL COLLECTION EFFORT: VERY HIGH

Requires advanced undestanding of specific network tools. Infiltration may require building trust with communities.

TYPE OF INTEL FOUND

Highly encrypted communication channels and marketplaces that cater to illegal activities

VALUE

Useful for tracking illegal activities and securing proprietary data.

DECENTRALIZED WEB PROJECTS (FREENET, ZERONET)

INTEL COLLECTION EFFORT: VERY HIGH

Requires specializied tools.
Monitoring activities requires continuous participation.

TYPE OF INTEL FOUND

- Websites offering discussions on sensitive topics
- Censored information or communications
- Development and exchange of tools

VALUE

- Useful for tracking illegal content.

COMMUNICATION CHANNELS (ENCRYPTED MESSAGING APPS)

INTEL COLLECTION EFFORT: VERY HIGH

Often requires social engineering, access to invitation-only forums, or real-time monitoring of encrypted channels.

TYPE OF INTEL FOUND

- Discussions on cyberattack coordination or tactics
- Trading of stolen data or illegal content
- Encrypted communications between criminal actors

VALUE

Critical for real-time threat detection, cybersecurity, and tracking disinformation campaigns or illegal activity coordination.
Offers early warning for organizations or law enforcement regarding impending attacks or fraud schemes.

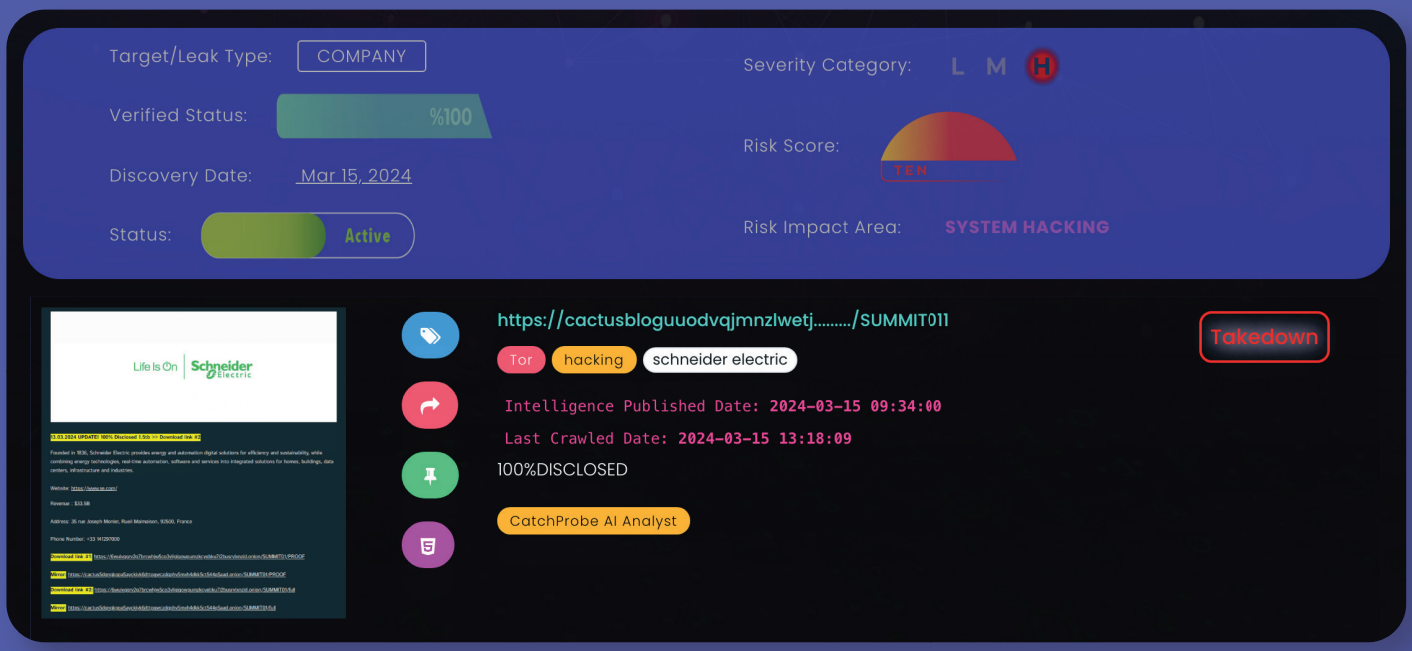
DARKMAP: Redefining Web Intelligence with AI and Next-Gen Capabilities

CatchProbe DarkMAP module enables precise. actionable intelligence across all layers of the internet facilitating advanced threat detection. analysis. and escalation for cybersecurity professionals.

Key Differentiators

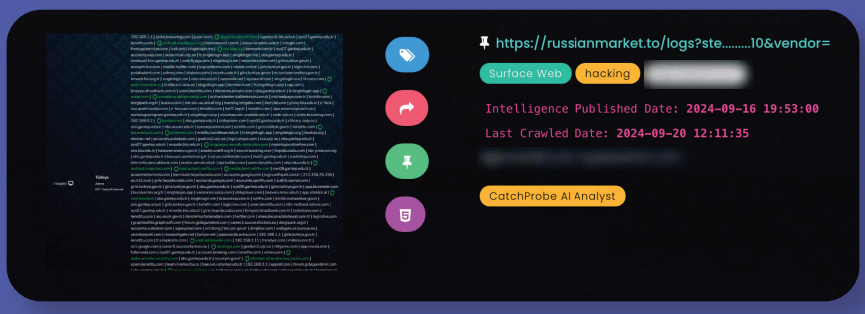
AI-Based Assessment:

DarkMAP's AI infrastructure assesses nndings in real time, generating detailed insights on threat severity, allowing for immediate prioritization and action.



Flow Management & Page Restriction Bypass:

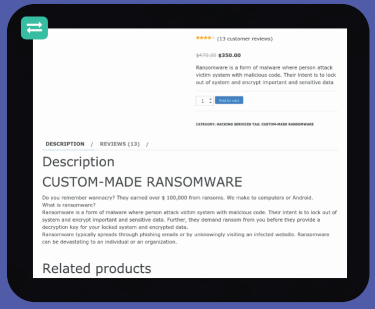
Capable of handling restricted or membership-based platforms, DarkMAP bypasses restrictions to ensure full data access across all layes of the web.



Additionally, DarkMAP can automatically acquire data within the pre-set budget allocated by CatchProbe.

Content Archiving

DarkMAP archives crawled data in screenshot format, ensuring future accessibility and documentation for retrospective analysis.



Additionally, if any changes are detected in the content after the initial crawl, users are alerted with a button in the top left corner.

OTD BİLİŞİM
GLOBAL VAD

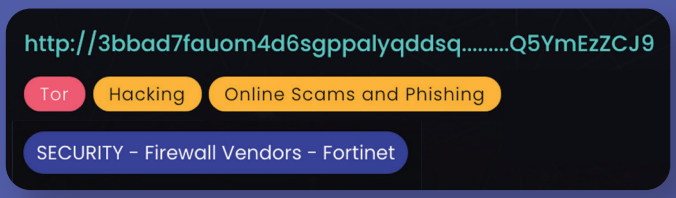
DarkMAP

Multilingual Translation

Not all threat intelligence data is in English-many threat actors operate using languages such as Russian, Korean, and others. DarkMAP automatically translates resources from these languages, enabling comprehensive, actionable insights across language barriers.

Vendor Research Without Limits

DarkMAP allows limitless tracking of vendors to monitor vulnerabilities, without any restrictions tied to license limits.



Automated and Manual Report

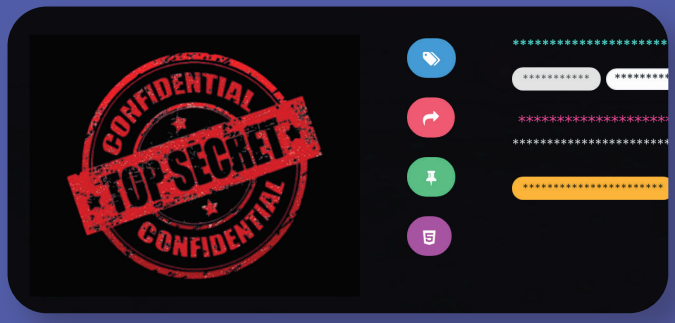
Users can conhgure automated email alerts in PDF format for new hndings, specifying when, how (e.g., based on risk score). and who should receive them.

Additionally, users can manually generate detailed reports directly from the module.

Escalation, Delegation, and Confidentiality

DarkMAP's platform architecture enables seamless delegation of tasks between teams and departments, optimizing workflow and collaboration.

Additionally, admins can set specihc information, such as subsidiary related keywords or executive names, to remain conhdential, ensuring only authorized personnel have access. Future related hndings are automatically protected, maintaining strict control over data.



OTD BİLİŞİM
GLOBAL VAD