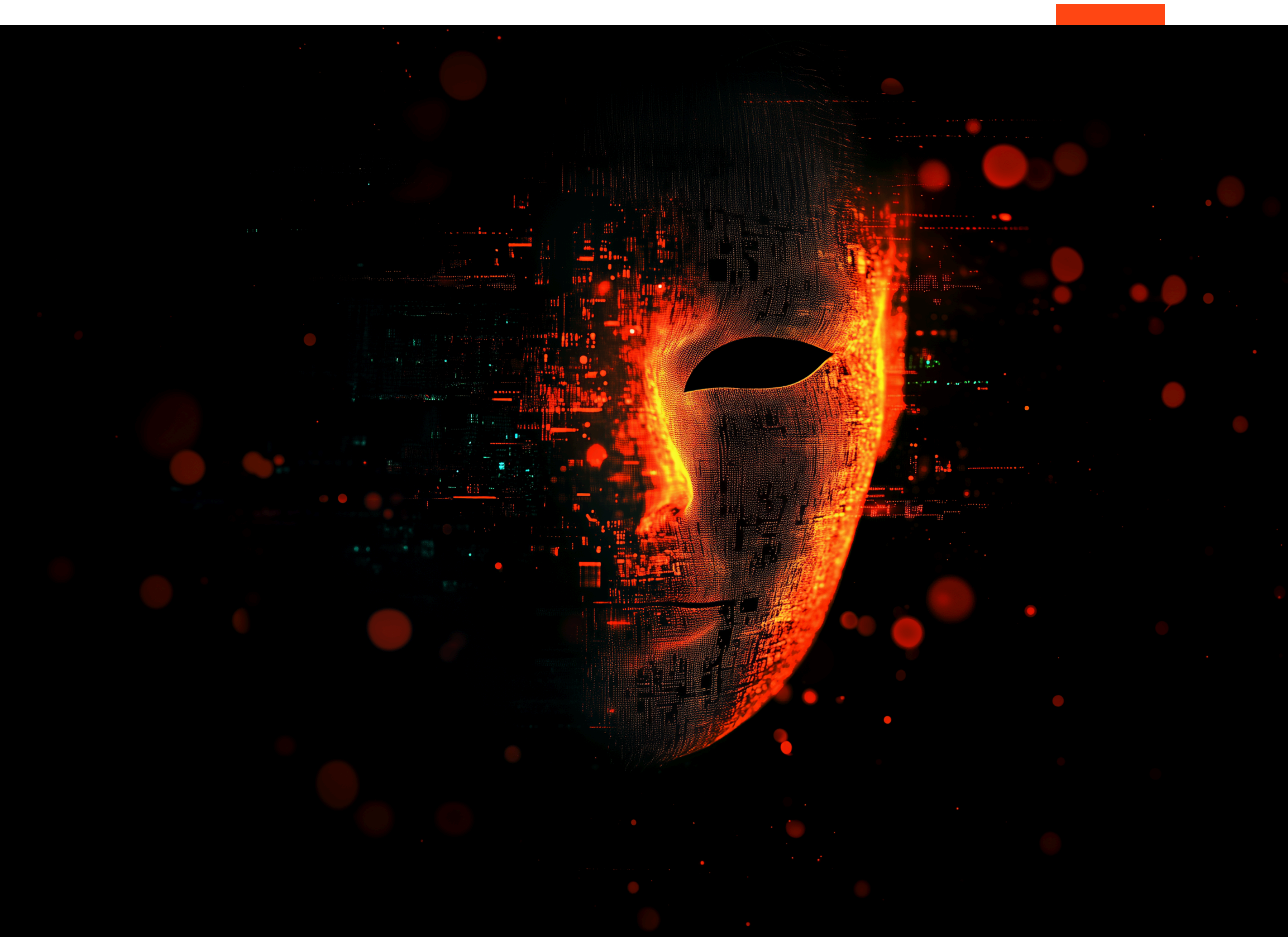
ORYXLABS

UNMASK

EXPOSING THE DARK SIDE OF ANONYMITY

PRODUCT BROCHURE



INTRODUCTION

In today's digital landscape, individuals seeking anonymity are increasingly using advanced tools like dark web sites, VPNs, cryptocurrencies, and social platforms. While these tools can be used for legitimate purposes, such as protecting privacy and freedom of expression, they can also be exploited by those with malicious intentions.

For decades, law enforcement and security agencies have faced challenges in identifying and tracking individuals who operate anonymously online.

A key factor contributing to the persistence of anonymity is the availability of sophisticated services. These services include complex systems with rotating IP pools, residential proxies, and P2P networks, which enable individuals to mask their identities and remain hidden. Additionally, encryption and traffic obfuscation techniques make it challenging for traditional security measures like Deep Packet Inspection (DPI) to detect their activities.

Moreover, individuals have developed network separation techniques, making it difficult to track their movements even when IP addresses are compromised. They operate in a realm where anonymity provides a layer of protection, and the consequences of undetected activities can be significant.

Because of this, we see the following trends:

» SOCIAL NETWORKS ARE BEING EXPLOITED

Social networks like Telegram, WhatsApp or Signal are being used by bad actors to communicate anonymously and share information.

» THE DARK WEB IS EXPANDING

The dark web, a subset of the internet that's intentionally hidden, is growing in size and popularity.

» ANONYMITY IS A SHIELD

The use of anonymous tools like VPNs, cryptocurrencies, and special social platforms make it impossible to track the identities of bad actors. This allows them to operate with impunity and evade detection.

2.5M+

Daily visitors to the dark web

90%

Of the internet comprises of deep and dark web

40%

Rise in decentralized platform use (Telegram)

$176M

Annual increase in ransomware cryptocurrency-based crimes on the dark web

2.95B

Monthly active users WhatsApp

950M

Monthly active users on Telegram

40M

Monthly active users on Signal

OUR SOLUTION

UNMASK is a de-anonymization engine that leverages deep domain expertise, Open-Source Intelligence (OSINT), network automation, and AI to generate the most comprehensive and accurate anonymity service IP feed available.

This powerful solution helps agencies stay ahead of evolving anonymity trends, ensuring they can identify and address potential threats effectively and with greater precision.

Our solution allows users to easily set up and deploy with only network logs in standard Netflow/IPFix format or any compatible format available.

We effortlessly detect and attribute hidden service owners and users and also social account profile owners, even in the presence of obfuscation and encryption, to disrupt and apprehend malicious actors.

The platform leverages OSINT and unique network watermarking technology to provide a comprehensive view of network activity, including onion sites and other malicious activities.

Based only on network log analysis, our **de-anonymization engine** provides unprecedented visibility to illegal online activities of network subscribers in the country.

» ACTIVITY DETECTION

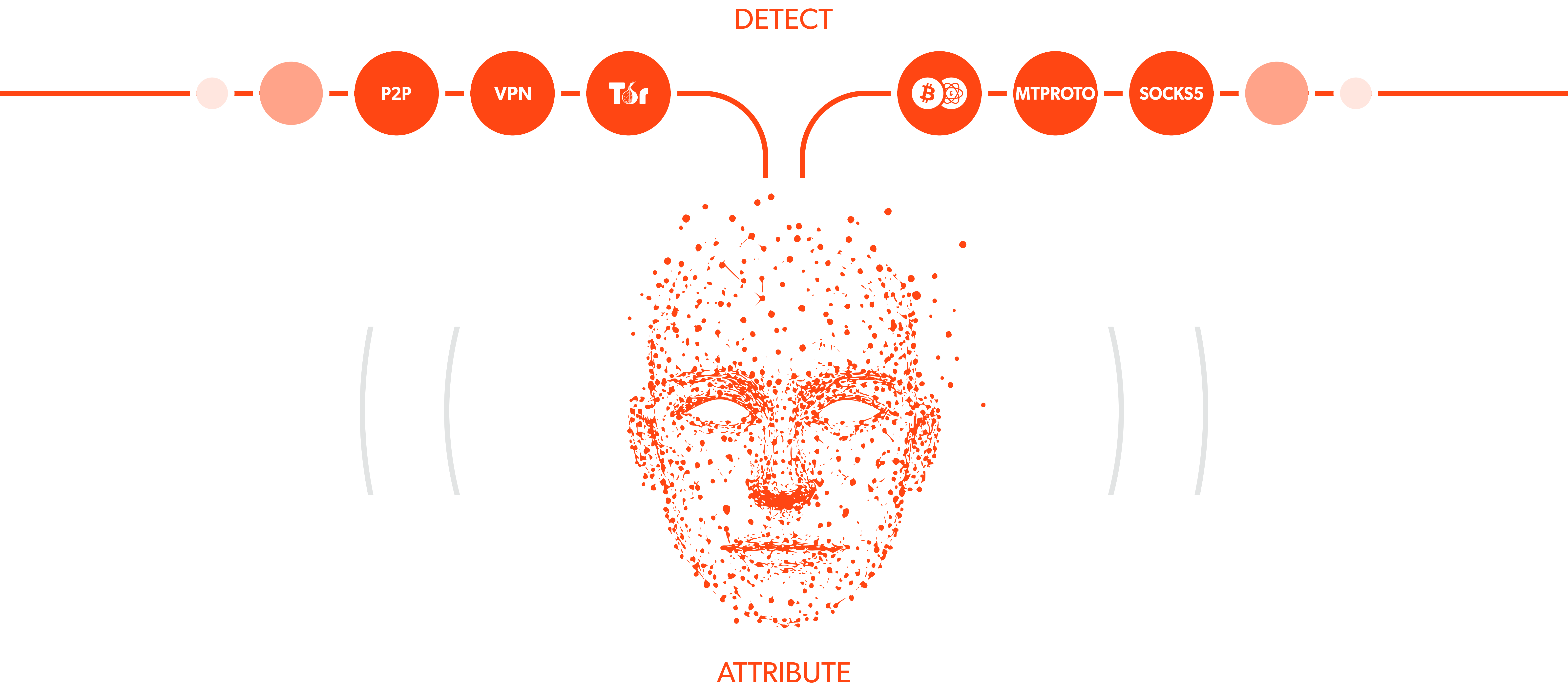
Detect suspects' network subscribers' access to thousands of different anonymity services and networks.

» TOR DE-ANONYMIZATION

Reveal Dark web (onion) sites operated or accessed by the suspects network subscribers.

» SOCIAL NETWORKING DE-ANONYMIZATION

Reveal suspects' network subscribers' Telegram, WhatsApp, Signal and Twitter(X) identities.



A key differentiator of the platform is the ability to **detect** all TOR traffic, including obfuscated ones and unpublished TOR bridges, Telegram proxies and more. We **attribute** selected hidden service users, providing unparalleled insights into anonymous activities. Our solution also reveals channel/hidden group administrators and subscribers – even when users remain silent.

By leveraging our unique features and benefits, **UNMASK** provides law enforcement and security agencies with a powerful solution to de-anonymize online activities with the ability to associate subscribers with sites they access and run, and associate social network suspects to their profiles.

FEATURES

UNMASK offers a range of unique features that set us apart from other cybersecurity solutions:

- **IDENTITY ATTRIBUTION CAPABILITIES**
  The de-anonymization capability helps attribute identities to individuals operating anonymously online.
- **ONION SITE DETECTION**
  Find any onion sites hosted in your network and select onion sites accessed by users or malware in your network.
- **ADVANCED CORRELATION ALGORITHMS**
  Use of advanced algorithms enable detection and attribution of anonymous online identities, even when obfuscated and encrypted.
- **OSINT CAPABILITIES**
  Leverages OSINT to gather information from publicly available sources, providing a comprehensive view of anonymous activities.
- **UNIQUE WATERMARKING TECHNOLOGY**
  Use of proprietary network watermarking technology allows for near real-time attribution of anonymous online activities.
- **NEAR REAL-TIME INSIGHTS**
  Offers near real-time attribution of anonymous online activities, enabling users to take swift action to safeguard their networks and assets.
- **ANALYSIS OF ENCRYPTED COMMUNICATIONS**
  The platform extracts unique insights for each network subscriber, including encrypted activity performed by the subscriber.
- **REQUIRES ONLY NETWORK LOGS**
  Our platform requires only network logs in standard Netflow/IPFix format or any compatible format as input.

BENEFITS

UNMASK provides numerous benefits to law enforcement and security agencies, including:

- **ATTRIBUTE ANONYMOUS ACTIVITIES**
  Attribute anonymous online identities and activities in near real-time, enabling our customers to identify hidden bad actors.
- **EFFORTLESS SETUP AND DEPLOYMENT**
  Easily set up and deploy with only network logs in standard Netflow/IPFix format or any compatible format required.
- **EXPOSE HIDDEN MALICIOUS SERVICES**
  Detect and attribute hidden service owners and users, even in the presence of obfuscation and encryption, to disrupt and apprehend malicious actors.
- **GAIN INSIGHTS INTO NETWORK ACTIVITY**
  Extract unique insights for each subscriber, including when network traffic is encrypted.
- **NEAR REAL-TIME THREAT RESPONSE**
  Attribute anonymous online activities in near real-time, enabling rapid response to emerging threats.
- **FULL VIEW OF NETWORK ACTIVITY**
  Leverage OSINT and unique watermarking technology for a comprehensive view of network activity, including social networks, onion sites and other hidden activities.

ORYXLABS

WHO WE ARE

ORYXLABS was founded in Abu Dhabi in 2020 with a passion for cybersecurity-focused engineering.

A proudly diverse staff hailing from 22 different countries with backgrounds ranging from national defense to world-renowned top software engineering organizations joined together to develop best-in-class security solutions.

We leverage research and innovation to provide solutions in four key areas:

- Cyber Security Assessment
- Monitoring
- Prevention
- Improvement

When combined, ORYXLABS solutions provide a holistic approach to situational awareness and attack mitigation.

WEBSITE

Scan to view

VIDEO

Scan to view

OUR MISSION

Our mission is to equip cybersecurity teams with first-in-class intelligence and technical solutions that continuously assess, monitor, and improve environments to mitigate ongoing or future attacks.

WHY US

As an agile and innovative company focused on cybersecurity, we pride ourselves on crafting highly tailored solutions to meet our clients' exact needs, not "one size fits all" products like our competitors in the domain.

With our combined experience in deep learning, AI, vulnerability research and big data, and partnerships with world-renowned subject matter experts, you can rest assured our solutions are built and run on information that is timely and accurate.

COMPANY AWARDS

2025

Most Innovative CyberSecurity Company

CyberSecurity Excellence Awards

2024

Most Innovative CyberSecurity Company

CyberSecurity Excellence Awards

2023

Most Innovative CyberSecurity Company

CyberSecurity Excellence Awards

2022

Top CyberSecurity Solutions Provider Middle East

Enterprise Security

ORYXLABS

21st Floor, Aldar HQ
Al Raha Beach
P.O. Box: 33289
Abu Dhabi, UAE

oryxlabs.ae