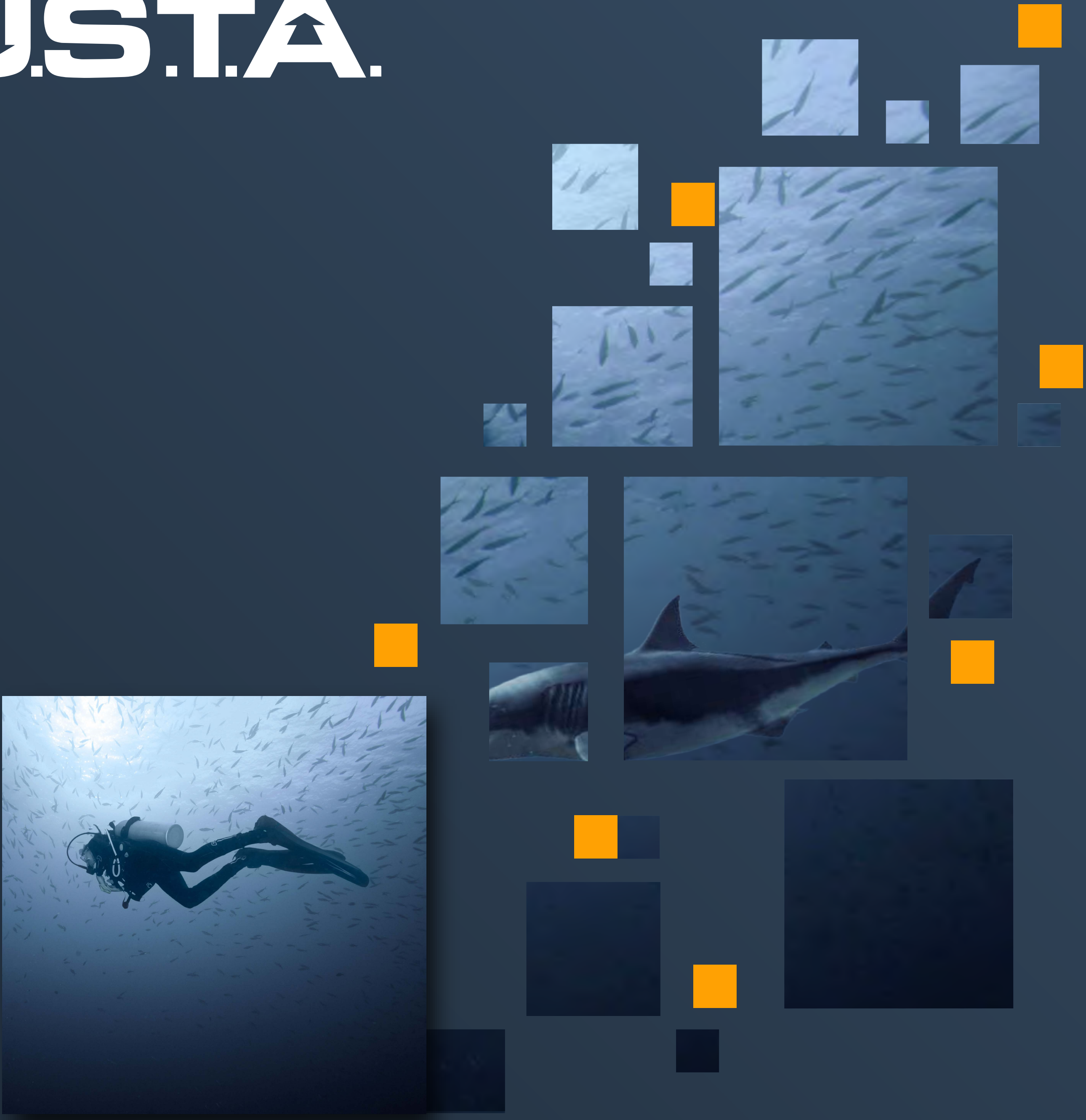
PRODAFT

THREAT INTEL & ANTI-FRAUD

U.S.T.A.



At **PRODAFT**, we provide client-specific intelligence to our customers and **in-depth analyses of the cybercrime groups through our U.S.T.A. platform**. As experts in our field, we help management to make intelligence-led decisions based on current techniques, tools, and behaviors of cybercriminals.

U.S.T.A. is **one of the first cyber threat intelligence platforms** ever developed. Our comprehensive intelligence-gathering cycle produces curated and verified threat reports that are relevant for your organization. For more than ten years, U.S.T.A. has been a trusted partner of hundreds of organizations with its unmatched capabilities.

CYBERSECURITY CHALLENGES

Cybersecurity is always shifting as new technologies emerge. Companies across all industries must safeguard their assets if they wish to move ahead securely and avoid losses. PRODAFT keeps its clients from the claws of cybercriminals or malicious threat actors.

Some industries are more susceptible to cyberattacks than others, and according to U.S.T.A.'s statistics, the most targeted industries in 2022 were: banking, fintech, aviation, defense, telecoms, eCommerce, energy, logistics, insurance, and public authorities.

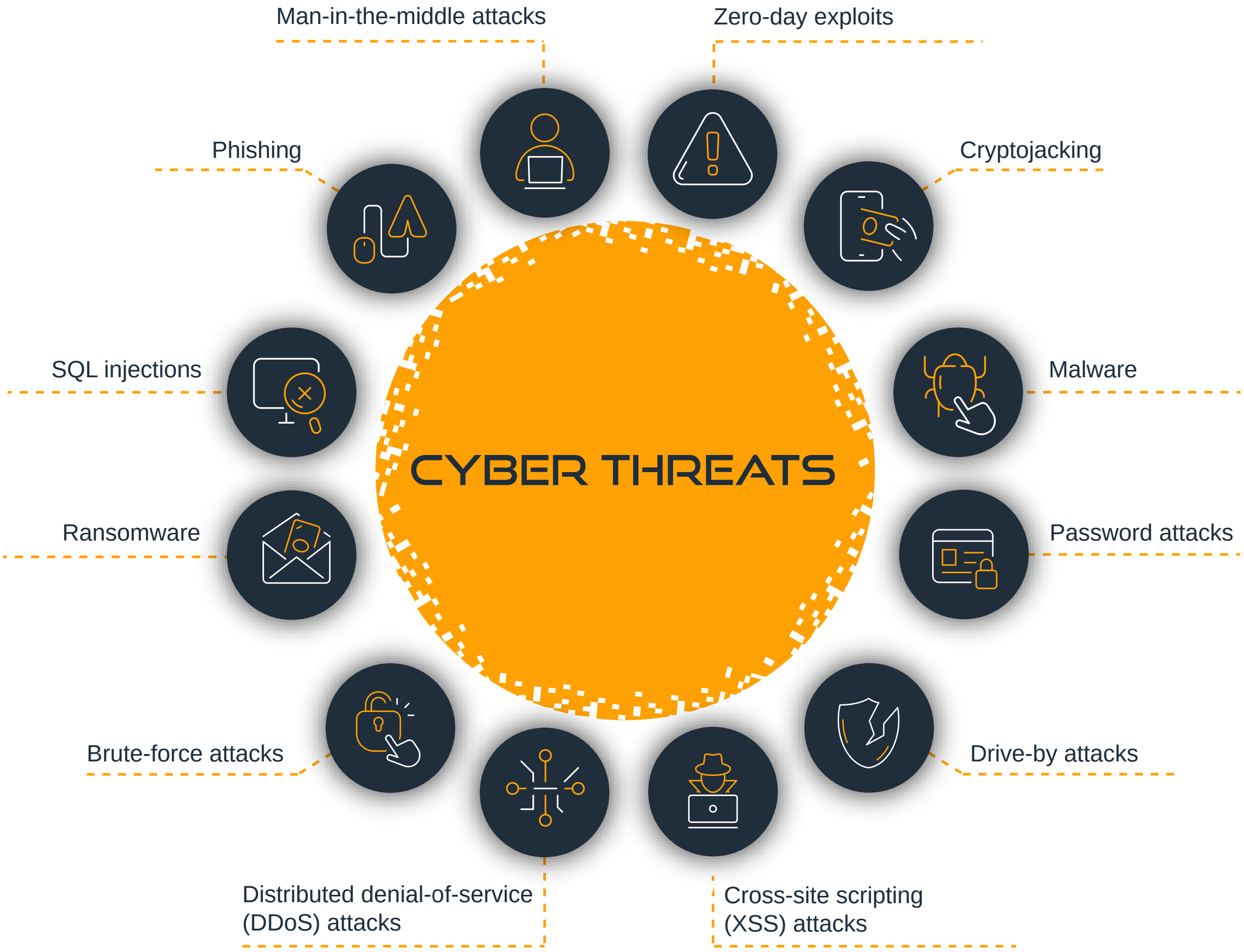
By 2025, 45% of organizations worldwide will experience advanced attacks on their supply chains.*

By 2024, organizations adopting a cybersecurity mesh architecture will reduce the financial impact of individual security incidents by an average of 90%. *

88% of boards now view cybersecurity as a business risk. *

**Source: Gartner Insights*

There are many different ways a threat actor can infiltrate a system. However, the most common types of cyberattacks include:



BEST PRACTICES TO PROTECT YOUR ORGANIZATION

Threat intelligence is essential for **every business and organization**, regardless of shape or size.

Small and midsize companies typically consider threat intelligence solely as a defensive position, dealing with the consequences once a cybersecurity incident has occurred.

Many businesses think that the cost of proactive curated intelligence is too high or that they are too small to be a target of cybercriminals. In addition, businesses are exposed to plenty of supply chain attack risks as a result of their suppliers, who are critical for the cybersecurity posture of their organization.

Not taking cybersecurity seriously has resulted in **significant losses** to their business. Everything can vanish in the blink of an eye due to a cyberattack, from business loss to investments, financial loss, and reputation damage.

By using a threat intelligence provider, businesses are able to make more informed decisions and enable them to be proactive in configuring their security.

U.S.T.A. CYBER THREAT INTELLIGENCE PLATFORM

Adopting PRODAFT's "Proactive Defense Against Future Threats" principle since Day 1, U.S.T.A. aims to provide its users with extremely clear and easy-to-interpret intelligence feeds.

THREAT INTELLIGENCE MODULE

Our **threat intelligence module** eliminates hard, manual data collection and provides timely and relevant insights about emerging cyber threats. Through the tailored reports your business receives, you will better understand threat actors, vulnerability trends, and attackers’ tools and accelerate your threat response.

FRAUD INTELLIGENCE MODULE

Banking institutions lose billions of dollars every year due to credit card fraud. Even more significant than the financial loss is the reputation damage and loss of customer trust. Our **fraud intelligence module** allows banking institutions to take a proactive approach and stop credit card fraud before it happens.

BRAND PROTECTION MODULE

Everything your brand consists of, including your customers, employees, executives, and products, must be safe from cyber threats. Our **brand protection module** helps your business protect against the threat actors that want to harm your brand using impersonations, phishing websites, compromised digital assets, etc.

In 2021, PRODAFT detected **2.5 million compromised credit cards** issued by 11’676 banks.

PRODAFT has detected **more than half a billion phishing campaigns** against U.S.T.A. members in the last five years.

KEY VALUES OF U.S.T.A.

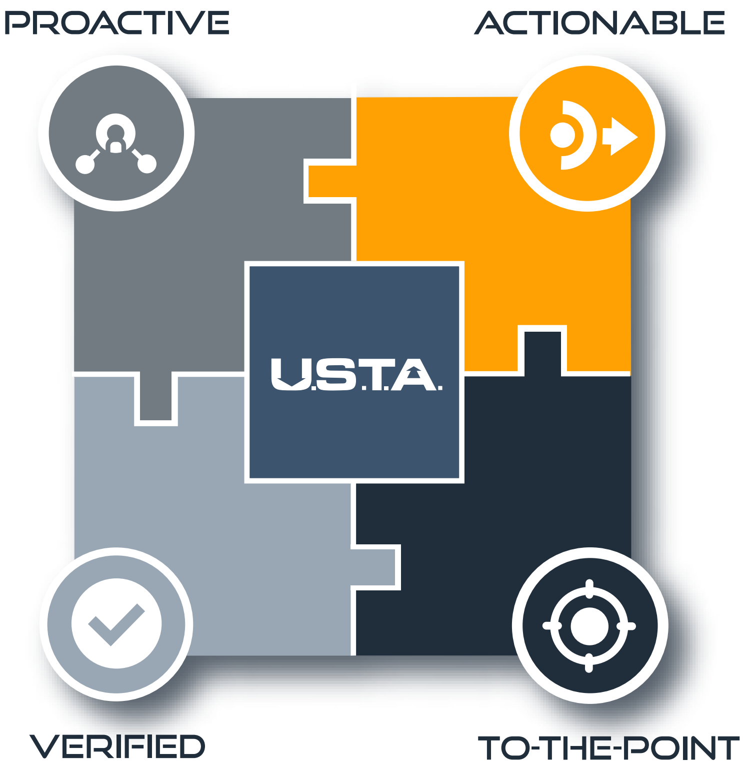
Each U.S.T.A. module has been developed according to the following principles:

Proactive

The most fundamental feature of the U.S.T.A. platform is its ability to provide timely information about potentially malicious threats. Thanks to its award-winning "Deep Web Sensors" technology, U.S.T.A. can warn clients of upcoming threats before evolving into harmful cyberattack incidents.

Actionable

Every U.S.T.A. platform notification serves a specific purpose and includes strict remediation. The U.S.T.A. cyber intelligence does all the heavy lifting, so users don’t have to conduct additional research or investigation. Thus, U.S.T.A. decreases the workload of its users while reinforcing their ability to combat cybercrime.



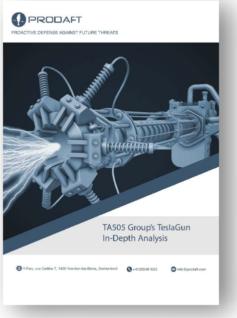
Verified

The threat intelligence data is verified to ensure our clients get highly accurate information they can count on. The analysts analyze each potential threat in detail with a well-defined HUMINT cycle.

To-the-Point

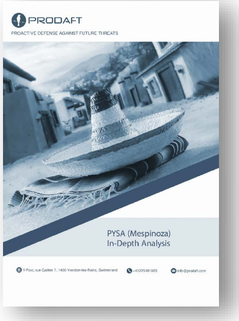
PRODAFT is diligent about addressing U.S.T.A. users' feedback, turning U.S.T.A. into a perfect solution that delivers what is needed. Our analysts strictly analyze and confirm the source of each threat before forwarding it to our users rather than forwarding it directly and expecting our users to figure out what to do.

ACTIONABLE INSIGHTS. RIGHT FROM THE SOURCE.

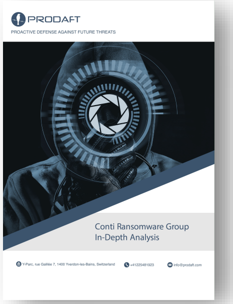


TA505 Group's TeslaGun

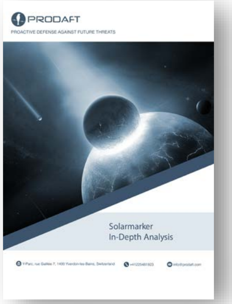
Wizard Spider Group



PYSA Ransomware Group



Conti Ransomware Group



Solarmarker Malware

FluBot Malware

Check Out Our Latest Reports

TAKEDOWN SERVICES

Cybercriminals are known for their talent for adaptation. When a new detection method is effective in discovering phishing sites, threat actors come up with new mediums of evasion to hide their phishing websites deeper and extend their lifespan.

Despite the contractual 48-hour guarantee, U.S.T.A.'s average takedown time has been ***2 to 4 hours*** in the last two years.

For this reason, PRODAFT's R&D team has constantly challenged itself to think one step ahead and design new detection methodologies for future evasion techniques.

The U.S.T.A. platform is reinforced with various different detection mechanisms (based on keyword, structure, image, and other similarities) that monitor the cyber-world to discover threat actors targeting U.S.T.A. member organizations.

U.S.T.A. is designed to decrease the workload of its users. Its services include phishing site detection and takedown and suspicious/malicious social media content detection and takedown, without requiring any request or interaction on the client side.

CYBERTHREAT REAL-TIME MAP

Discover the cyber threats happening in the world in real-time with our online tool.

On the map, you will find the following information about cyber threats:

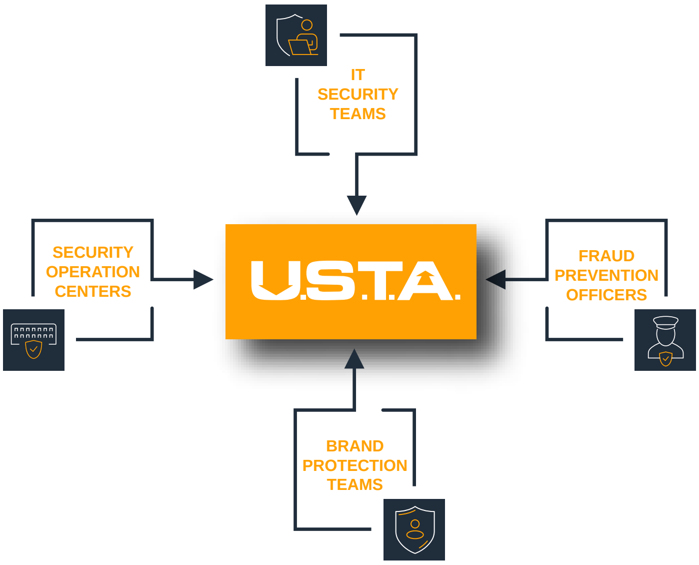
- Threat type
- IP Address
- Country
- Source map
- Timestamp

WHY THREAT INTELLIGENCE MATTERS TO YOUR ORGANIZATION

As a result of our solutions' **customized approach**, PRODAFT's client turnover is virtually nil, as we recognize the priorities and requirements unique to each industry.

U.S.T.A. is used by many teams across the globe. With different hierarchical authority levels and management options provided, different teams can benefit from U.S.T.A.'s cyber threat intelligence services on behalf of multiple clients managed by their teams.

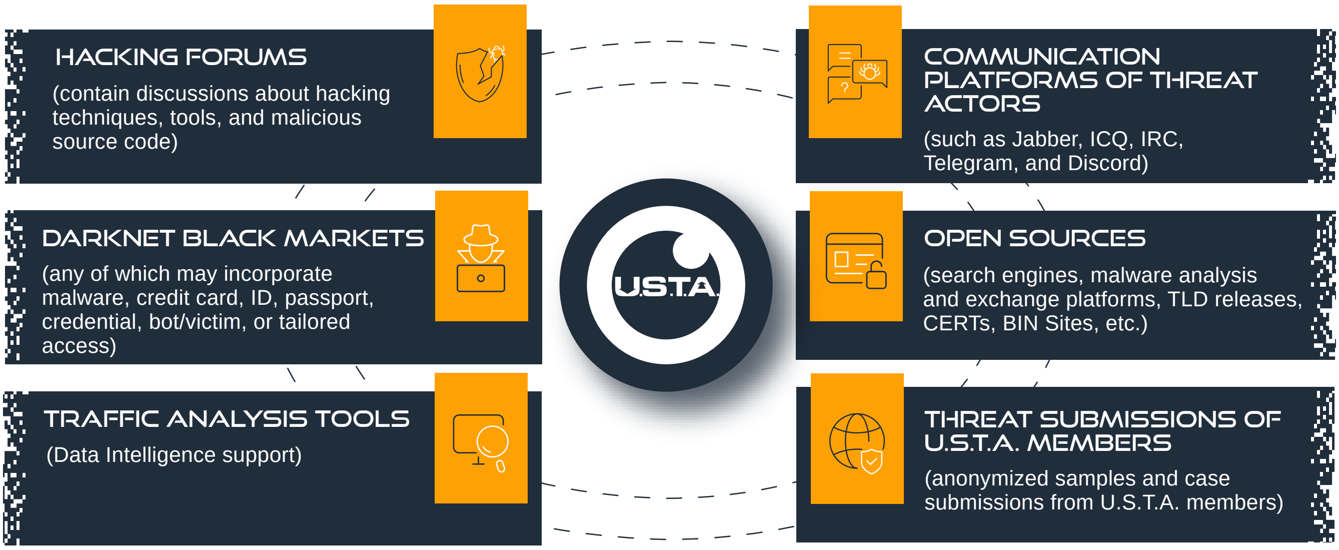
All the following rely on U.S.T.A. to discover and analyze threats in their domain:



EYES ON THOUSANDS OF SOURCES

To meet the challenges of complex cyberattacks, U.S.T.A. is reinforced with dozens of intelligence collection tools that monitor thousands of sources.

U.S.T.A. monitors different aspects and areas of various deep web, dark web, and clear web platforms to observe these constantly changing landscapes better. To remain undetected among these communities of threat actors, our team members have developed personas that have been active on these channels for years.



HACKING FORUMS

(contain discussions about hacking techniques, tools, and malicious source code)

DARKNET BLACK MARKETS

(any of which may incorporate malware, credit card, ID, passport, credential, bot/victim, or tailored access)

TRAFFIC ANALYSIS TOOLS

(Data Intelligence support)

COMMUNICATION PLATFORMS OF THREAT ACTORS

(such as Jabber, ICQ, IRC, Telegram, and Discord)

OPEN SOURCES

(search engines, malware analysis and exchange platforms, TLD releases, CERTs, BIN Sites, etc.)

THREAT SUBMISSIONS OF U.S.T.A. MEMBERS

(anonymized samples and case submissions from U.S.T.A. members)

STRUCTURE AND OPERATION

1. Structure

U.S.T.A. works as a web-based platform that requires no on-site installation or configuration. Our clients aren't asked to provide any confidential information before or during their experience with U.S.T.A. Likewise, U.S.T.A. does not conduct any vulnerability assessment or similar active footprinting procedure on the systems of its users to acquire information.

U.S.T.A. has four main modules that address the requirements of different personnel in an organization:

TACTICAL INTELLIGENCE

- Custom Threat Reports (featuring incidents or trends that affect the receiving U.S.T.A member, its industry, or region.

SECURITY INTELLIGENCE

- Custom Malware Analysis Reports
- Vulnerability Notifications
- U.S.T.A Leak Database
- Stolen Corporate Credentials Notifications (botnet intelligence)

FRAUD INTELLIGENCE

- Stolen Credit Card Notifications (for banking institutions)
- Fraud Method Notifications
- Stolen ID and Passport Feeds
- Stolen Customer Credential Notifications

BRAND PROTECTION

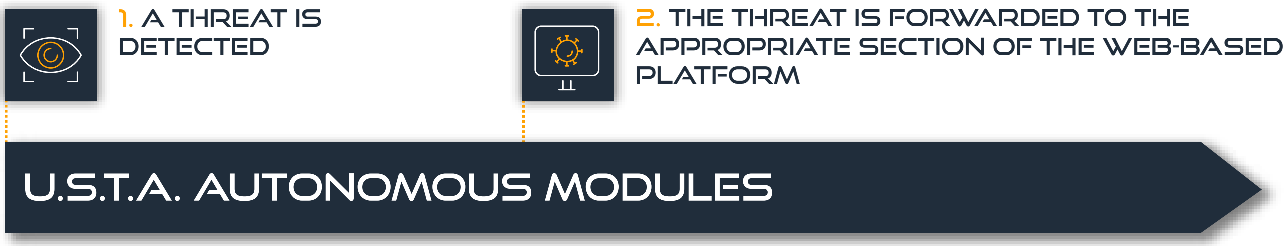
- Phishing Site Detection and Takedown
- Suspicious / Malicious Social Media Content Detection and Takedown

2. Operation

Autonomous Modules

Some U.S.T.A. platform features are autonomous and work without any analyst's interception.

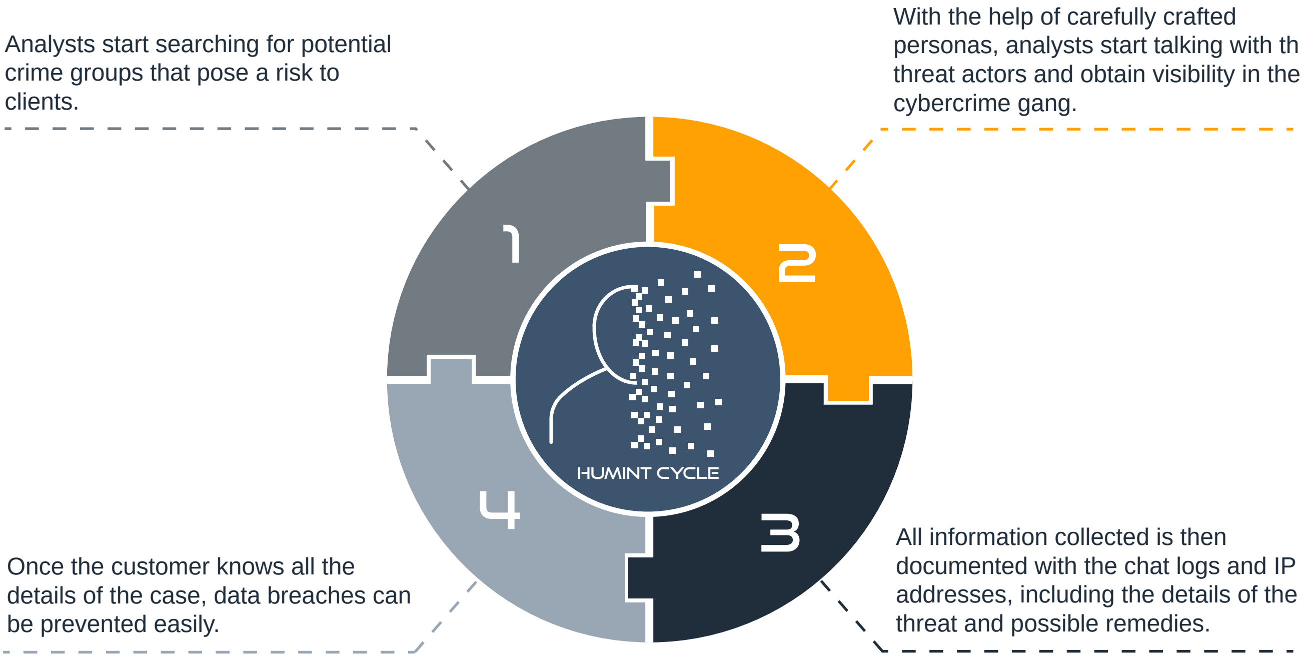
U.S.T.A. members can log in to our platform to browse these feeds and take advantage of U.S.T.A.'s API integrations directly into their security infrastructure.


1. A THREAT IS DETECTED
2. THE THREAT IS FORWARDED TO THE APPROPRIATE SECTION OF THE WEB-BASED PLATFORM
U.S.T.A. AUTONOMOUS MODULES

U.S.T.A. Advanced Analysis Feeds (Detect, Analyze, and Forward)

Several feeds of U.S.T.A. are Advance Analysis Feeds (AAF). These feeds feature threats discovered by U.S.T.A. Dark Web Sensors (crawlers and traffic analyzer tools).

U.S.T.A. ADVANCED ANALYSIS FEEDS



Analysts start searching for potential crime groups that pose a risk to clients.

With the help of carefully crafted personas, analysts start talking with the threat actors and obtain visibility in the cybercrime gang.

All information collected is then documented with the chat logs and IP addresses, including the details of the threat and possible remedies.

Once the customer knows all the details of the case, data breaches can be prevented easily.

PRODAFT TEAM

Regardless of the technological means available, becoming a successful solution provider in cybersecurity is only possible by the efforts of a multidisciplinary team, where each member possesses years of focus in a chosen field.

PRODAFT has a talent pool of multicultural and multidisciplinary cybersecurity experts who have published groundbreaking research papers in their respective areas. Our highly dedicated cybersecurity professionals have the specialized training, certification, knowledge, and skills to produce actionable and valuable insights.