PRODAFT

# THREAT INTEL REDEFINED

# U.S.T.A.

PRODAFT was founded as a cyber threat intelligence company in 2012. Aimed at creating a difference through expertise, the brand has significantly evolved thanks to its apposite technologies, all of which are developed in-house.

By looking at cyber threats from a realistic perspective PRODAFT has always positioned itself as a "professionally unconventional" provider in its field, thanks to a suite of proprietary solutions. PRODAFT continues to serve a range of global brands and critical industries via its threat intelligence, penetration testing, and security research teams.

"To ensure the proactive nature of PRODAFT's solutions, our operational cycles are constantly reviewed and adapted to emerging challenges within the cyber arena. Owing to this state of flux, PRODAFT is always prepared for the new realities and challenges of cyber security. Our clients will never find themselves blindsided by any newly evolving cyber trend.

## CLIENT PORTFOLIO

Since 2012, PRODAFT has been a key solution provider for various critical sectors,including banking and finance, fintech, aviation, insurance, IoT (customer tech), defense, and telecommunication.
Due to the "customized" approach of our solutions, PRODAFT's client turnover is virtually nil, as we recognize the priorities and requirements unique to each industry.

## TEAM

Regardless of the technological means and mediums available, becoming a successful solution provider in security is only possible by the efforts of a multi-disciplinary team, every member of which possesses years of focus in a chosen field.
That's why PRODAFT has a talent pool consisting of more than 40 globally recognized specialists who have published groundbreaking articles in their respective areas of concentration.

# USTA CYBER THREAT INTELLIGENCE PLATFORM

Continuously growing since 2012, U.S.T.A. is one of the first cyber intelligence platforms ever developed. Featuring a unique synergy of threat intelligence, fraud intelligence and brand protection modules; USTA responds directly and effectively to today's complex cyber threats.

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

Aside from its autonomous features, U.S.T.A. is supported by PRODAFT's globally recognized threat intelligence, security research, and malware analysis teams, which continuously respond to every threat discovered.

## U.S.T.A. proudly serves following the critical infrastructures:

- BANKING AND FINANCE
- FINTECH
- AVIATION
- DEFENSE
- TELECOMMUNICATION
- E-COMMERCE
- ENERGY
- LOGISTICS
- INSURANCE
- PUBLIC AUTHORITES

Primarily used by incident response, security operations, fraud prevention and brand protection teams in critical infrastructures, each U.S.T.A. module has been developed according to the following set of key principles.

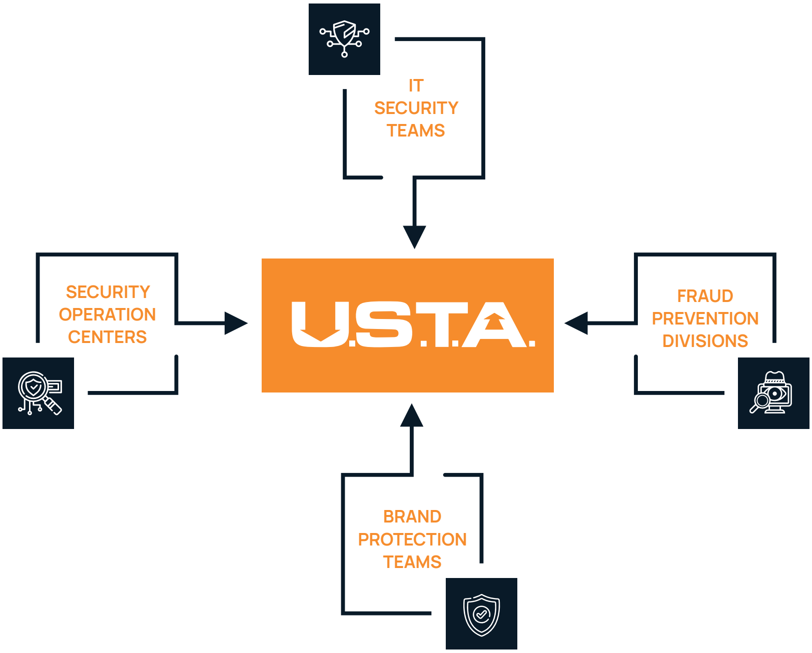
# KEY VALUES OF U.S.T.A.

● **Proactive:** The most fundamental feature of U.S.T.A.'s cyber intelligence platform is its ability to provide timely information about potentially malicious threats. Thanks to its award-winning "Deep Web Sensors" technology, USTA can warn security operation, fraud prevention, and/ or brand protection teams of upcoming threats before they evolve into harmful cyber-attack incidents.

● **Actionable:** every U.S.T.A. platform notification serves a specific purpose and includes strict remediation. Our users benefit from the added value of having U.S.T.A. as a cyber intelligence platform rather than needing to conduct additional research or investigation. Thus, U.S.T.A. decreases the workload of its users while reinforcing their ability to combat cybercrime.

● **To-the-Point:** Since its first release in 2012, PRODAFT has been very diligent about addressing the feedback of U.S.T.A. users, turning U.S.T.A. into a perfect solution that **delivers** exactly what's 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 tofigure out what to do.

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

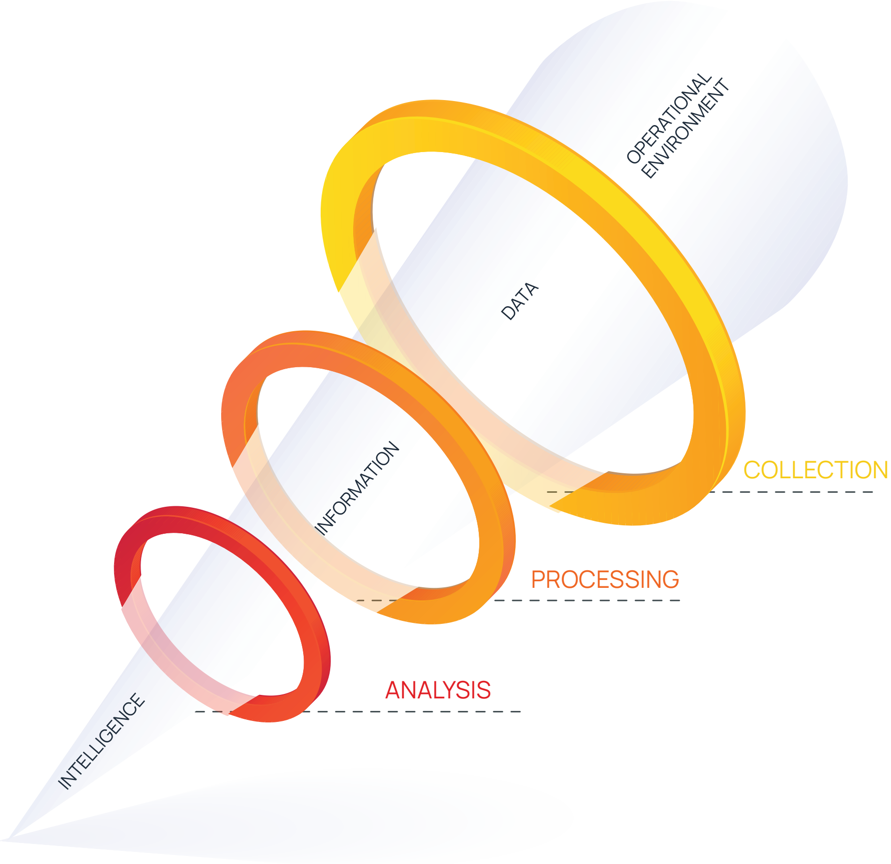


# TRUE INTELLIGENCE

Unfortunately, today's world of cyber intelligence (or cyber-threat intelligence) has lost track of what constitutes "intelligence" due to the challenges of the intelligence collection lifecycle.

Even though gathering cyber threat intelligence is a difficult and complex process, U.S.T.A. has always insisted on providing distilled information based on several different analysis procedures rather than solely relying on "keywords."

Our users always receive a detailed notification or report about a threat that depicts the source, impact, and severity of the case based on different human intelligence, open-source intelligence, or signal intelligence (via U.S.T.A.'s Deep Web Sensors) procedures tailored to the matter being investigated.



# EYES ON EVERY SOURCE

To meet the challenges of today's complex cyber-attacks, U.S.T.A. is reinforced with dozens of intelligence collection tools that monitor thousands of different sources.

As each cyber threat type requires a different monitoring approach, U.S.T.A.'s tracking tools and intelligence sources vary according to different types of threat, including but not limited to:

- Targeted attacks against U.S.T.A. member organizations such as advanced persistent threats, zero-day vulnerabilities, and spear-phishing campaigns

- Generic/indirect attacks against U.S.T.A. member organizations such as ransomware threats, phishing campaigns, and stealer malware

- Targeted and generic attacks against clients of U.S.T.A. member organizations such as Malware-as-a-Service and Ransomware-as-a-Service campaigns, stealer botnets, or phishing sites

- Out-of-band attacks, such as malicious social media campaigns or fake mobile applications, that damage the reputations of U.S.T.A. members

U.S.T.A. monitors different aspects and areas of various deep-web, dark-web, and clear-web platforms to better observe these constantly changing landscapes.

**CYBER ATTACK / HACKING FORUMS**

**COMMUNICATION PLATFORMS OF THREAT ACTORS**
Actors (such as Jabber, ICQ, IRC, Telegram, and Discord)

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

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

**TRAFFIC ANALYSIS TOOLS**
(back-end SIGINT support)

**THREAT SUBMISSIONS OF USTA MEMBERS**
(anonymized samples and case submissions from other 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 are never asked to provide any confidential information prior to, or during, their experience with U.S.T.A. Likewise, U.S.T.A. does not conduct any vulnerability assessment or similar active foot-printing procedure on the systems of its users to acquire information.

U.S.T.A.'s operation is designed to collect and acquire proactive threat intelligence from external cyberspace before our clients are put in harm's way.

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 affects 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 Credential Notifications (botnet intelligence)

### FRAUD INTELLIGENCE

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

### BRAND PROTECTION

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

# STRUCTURE AND OPERATION

## 2.Operation

### Autonomous Modules (Detect and Forward)

The following feeds of U.S.T.A. are autonomous. These modules work without any analyst's interception:

- **Stolen Credit Cards (for banking institutions)**
- **Stolen Corporate Credentials (botnet intelligence)**
- **Social Media Malicious Content Detection**
- **Phishing Website Detection**
- **Stolen Client Account (clients of U.S.T.A. members)**
- **Stolen ID and Passport Notifications**
- **U.S.T.A. Leak Database**

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

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

The following feeds of U.S.T.A. are Advance Analysis Feeds (AAF).

- **Tactical Intelligence**
- **Vulnerability Intelligence**
- **Malware Intelligence**
- **Fraud Method Intelligence**

These feeds feature threats that are discovered by U.S.T.A. Dark Web Sensors (crawlers and traffic analyzer tools) in the background.

When a U.S.T.A. member's name, IP, or other identifying information is detected in the Dark Web, the issue is directly forwarded to our team of analysts.

**• U.S.T.A. never sends such threats without prior analysis to mitigate the chances of false positives.**

U.S.T.A. relies on a talent pool of 40 analysts who are recognized experts in their fields. These analysts examine and inspect these findings and conduct further research (e.g., human intelligence, open-source intelligence, or security risk assessment) on the matter. The findings of our analysts are then forwarded to the appropriate section of the web-based platform in either "notification ticket" or "case report" format.

## COMPLETE BI-DIRECTIONAL SUPPORT IN ALL MODULES

Nobody knows a corporation’s actual needs and requirements better than its team. That’s why U.S.T.A. is operated in a bi-directional manner.

Under the scope of U.S.T.A.’s cyber intelligence services, our teams do not only detect and terminate the threats that our systems find, but also respond to the threats which have been sent by the teams of our users. This way, users can guide U.S.T.A. analysts according to their specific requirements.

## COMPLETE API INTEGRATION

Aside from its intelligence feeds, U.S.T.A. also enables its users to receive IOC ("indicators of compromise") feeds about various types of threats in their desired format.

Users of U.S.T.A. can simply log in to the API management section of our platform and choose their desired type and format of API feed from the multiple options provided.

## U.S.T.A. FOR SOCS

U.S.T.A. is also used by different remote security operation centers (SOCs) across the globe. With different hierarchical authority levels and management options provided, SOCs can benefit from U.S.T.A.’s threat intelligence services on behalf of multiple clients managed by their teams.

## CORPORATE USER MANAGEMENT AND REPORTING

Since 2012, U.S.T.A.'s main clients have always been multinational corporations. This deep professional experience has enabled PRODAFT to transform U.S.T.A.'s user interface and authority management features in a way that perfectly complies with corporate requirements. On U.S.T.A.'s web-based platform, decision-makers of a company can customize their weekly reports and manage the activities of users in separate branches.

PRODAFT

Eyes on every source