VERIFIED INTELLIGENCE

Eliminate noise - use verified intelligence

PRODAFT

Today's security professionals face a constant flood of "partially relatable" threat alerts and notifications from multiple vendors.

- The U.S.T.A. threat intelligence platform automatically **dissects, verifies, and investigates threats** before sending them to you.
- U.S.T.A. uses **human and data intelligence** to verify alerts and provide customers with curated, high-priority threat data.

Each of these threat alerts must be handled on a case-by-case basis. The non-stop flow of unverified alerts creates a highly demanding workload for security event response personnel and their teams.

Currently, PRODAFT has neutralized ***3'885'374 threats***, which directly targeted our client portfolio.

The U.S.T.A. threat intelligence platform reduces the time and energy spent on analyzing, interpreting, and verifying potential outsider threats. It gives security operatives on-demand insight into threat profiles on an individual basis.

The combination of automatic and manual processes lets users glean valuable insight about cyber threats directly through a single dashboard. Users can:

- Discover the nature of the threat.
- Identify its origin and known information about the threat actor behind it.
- See the source of detection alongside information about that source.
- Predict the likelihood of compromise based on previous data acquired from the same threat actor.
- Obtain Proof of Value, Proof of Concept, or related sample data from the threat actor responsible.
- Determine the potential impact of the threat, and evaluate probable targets.

THREAT VERIFICATION

Reduce risk with Verified Alerts

PRODAFT

U.S.T.A. uses two types of intelligence to verify alerts and provide customers with curated, high-priority threat data:

1

Human Intelligence

U.S.T.A. combines award-winning dark web sensors with the insight of a skilled team specifically trained to identify and categorize security threats. Tactical intelligence notifications are reinforced with detailed analysis crafted by a human intelligence team. Human intelligence is one of the most valuable capabilities PRODAFT operators offer.

U.S.T.A. operators combine threat intelligence expertise with Russian, Turkish, German, and English native-level language skills. They use highly reputable PRODAFT personal accounts with an excellent reputation on hundreds of underground platforms. These operators play a crucial role in acquiring knowledge about threats and threat actors from the other side of the fence.

2

Data Intelligence

Once the team detects a threat actor is exploiting a specific vulnerability or operating a particular Command and Control Server, U.S.T.A. operators can begin verifying the threat's validity using U.S.T.A. traffic analysis tools.

PRODAFT operators use these tools to collect network fingerprints associated with the threat. This enables further investigation to form a better understanding of the threat or uncover the techniques and tactics threat actors use. This is how operators infiltrate Command and Control servers and identify malicious URLs associated with cybercrime groups.

Since 2012, PRODAFT has offered customized and proactive defense against constantly evolving cyberattack techniques. Our cyber threat intelligence platform, U.S.T.A., is a key solution for various critical sectors, including banking and finance, e-commerce, fintech, aviation, insurance, IoT, defense, and telecommunication. Thanks to our unique synergy of tactical intelligence, fraud intelligence, brand protection and security intelligence, we provide actionable, proactive and to-the-point intelligence feeds to prevent threats before they evolve into harmful cyberattack incidents.