PRODAFT

CASE STUDY

ADVANCING THE CAPABILITIES OF A MAJOR SOC PROVIDER WITH OUR THREAT INTELLIGENCE SOLUTIONS

Industry: IT

Region: MENA Region

Challenge: Integrating next-gen threat intelligence solutions for SOC clients operating in different verticals

Who is the Client?

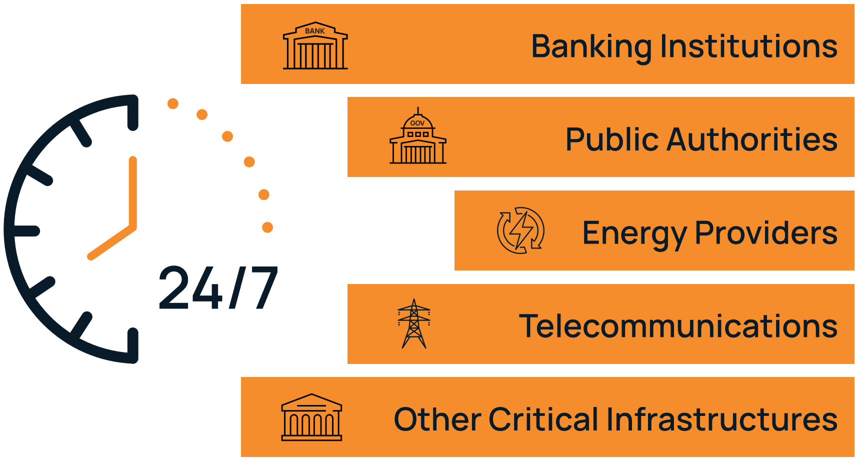
One of the leading IT companies in the MENA region with;

80 years of business experience

2’000+ employees

80+ international partnerships

The organization’s 24/7 security operations center (SOC) provides critical infrastructure to banking institutions, public authorities, energy providers, and telecommunications companies, among others.



The organization’s 24/7 security operations center

The SOC provider identified PRODAFT’s U.S.T.A. threat intelligence platform as an appropriate solution for proactive defense against evolving cyber threats.

What Was The Main Challenge?

The SOC provider wished to consolidate its reputation as one of the most valuable brands in its sector by offering next-generation threat intelligence services to Remote Security Operation Center clients.

Since the clients came from a wide array of verticals, it was necessary to find the best security approach for each of their individual challenges and to meet their requirements in alignment with the business objectives.

Why Did They Reach Out To Us?

The SOC provider reached out to us and explained its motivation for offering proactive threat intelligence service to their customers.

Its team underscored the importance of enhancing the security services it offers to customers, with multiple service level tiers that correspond to the customer’s industry, security orchestration, and maturity. Due to its versatility and intelligence-led data, the SOC provider identified our U.S.T.A. Threat Intelligence platform as an appropriate solution for proactive defense against evolving cyber threats.

How Did We Proceed?

After signing a mutual protocol and non-disclosure agreement, the SOC provider shared its portfolio with us. It contained a variety of organizations, from mid-sized businesses with no dedicated security personnel to enterprise-level organizations with dedicated on-site security operations centers.

Each customer had its own tech stack and unique security requirements. Successful deployment of threat intelligence capabilities required case-by-case implementation for each organization. While some customers needed threat intelligence data fed to internal systems via API, others focused on fraud intelligence reports or brand protection (anti-impersonation) services.

What Were The Solutions?

The necessary steps towards a successful solution were two-fold:

1

We assessed the scope of the client's remote SOC management service. This allowed our PRODAFT team to identify which APIs can be utilized for bridging the ThreatStream API feed of its U.S.T.A. platform to the client's customers. Careful API deployment ensured a seamless transfer of valuable security data like Indicators of Compromise (IoCs) to customer endpoints.

2

We developed a comprehensive service model for organizations that lacked security expertise. These organizations were not able to interpret threat notifications and reports without a “Managed Threat Intelligence & Response” service, or a series of educational USTA workshops designed to introduce the platform to end-users.

Afterwards, together with the SOC provider, we offered both solutions to their customers:

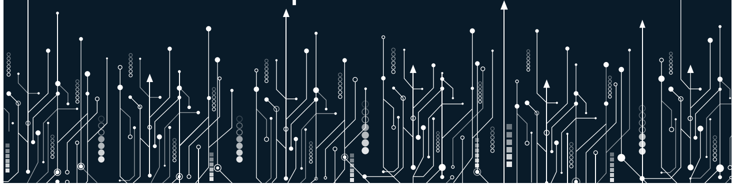
Ultimately, **PRODAFT** and **SOC provider** offered both options to customers:

- A SOC-level management section was developed for the U.S.T.A. platform, enabling the client to offer Managed Threat Intelligence & Response as a service. This allowed the SOC personnel to access, visualize, and respond to threat notifications for multiple organizations through a centrally managed dashboard.
- U.S.T.A. Threat Intelligence workshops were provided to end-users who needed to access and mitigate threats on their own behalf. This solution empowered the client’s mid-sized customers to expand their expertise and improve security performance.

What Was The Outcome?

Both efforts were thoroughly planned and successfully applied. We worked together with the SOC provider to mitigate the risk of end-customers succumbing to novel cybercriminal attacks using comprehensive threat intelligence services, reinforced with collaborative blue-team activities.

> With our help, the SOC provider acquired an important competitive advantage over other remote SOC-as-a-service providers.



Over the past two years, it has successfully enabled the sale and provision of threat intelligence services to more than 70 customers. During this time, the collaboration has been generating positive returns, along with zero negative feedback and is on track for constant renewal.

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.